
IP-verkkolaitteiden konfiguraationhallinta Corenet Oy:n liiketoiminnassa



Ammattikorkeakoulun opinnäytetyö

Tietotekniikka

Riihimäki, syksy 2013

Tommi Bäckman



Riihimäki
Tietotekniikka
Tietoliikennetekniikka

Tekijä	Tommi Bäckman	Vuosi 2013
Työn nimi	IP-verkkolaitteiden konfiguraationhallinta Corenet Oy:n liiketoiminnassa	

TIIVISTELMÄ

Corenet Oy on pieni suomalainen operaattori ja integraattori, joka on erikoistunut toteuttamaan asiakkailleen tietoliikenteen erikoisratkaisuja. Corenet Oy:llä on hallinnoitavanaan tuhansia omia ja asiakkaiden verkkolaitteita.

Työn tavoitteena oli etsiä Corenet Oy:n tarpeisiin sopiva verkkolaitteiden konfiguraationhallintatyökalu, jonka avulla suoritettaisiin konfiguraatioiden automatisoitu luominen, tarkistaminen ja talteenotto. Työkalulla tulisi myös voida suorittaa laitteiden massakonfigurointi.

Työ aloitettiin laatimalla kysely Corenet Oy:n asiantuntijoille. Kysely luotiin Microsoft Sharepoint -järjestelmällä. Kysely suunnattiin kaikille työntekijöille, joita tämä uusi työkalu koskettaisi. Kyselyyn saatiin vastausten lisäksi myös tärkeitä kommentteja ja kehitysehdotuksia.

Seuraavaksi työssä keskityttiin laatimaan kyselyn pohjalta vaatimusmäärittely. Vaatimusmäärittelyn sekä pisteytysmenetelmän avulla kilpailutettiin vaihtoehdot. Kilpailutuksen perusteella on tarkoitus valita sopivin työkalu Corenetin tarpeisiin, joko valmiista kaupallisista työkaluista tai avoimen lähdekoodin työkaluista.

Työssä käytettiin hyväksi haastattelujen, kokemuksen ja kommenttien lisäksi myös kaikkea saatavilla olevaa tietoa lähinnä Internetistä, mutta myös kirjoista ja koulutustilaisuuksista saatua tietoa sekä valmistajien antamia tietoja.

Työ eteni suunnitelmien mukaisesti siihen pisteeseen, että Corenet voi suorittaa käytännön testejä työkalulle ja sen jälkeen tehdä valintapäätöksiä. Lopullista valintaa tai soveltuvuustestausta ei tässä työssä käsitellä, vaan se käsitellään Corenetilla sisäisesti.

Avainsanat Konfiguraationhallinta, verkonhallinta, hallintatyökalu, Open Source

Sivut 32 s. + liitteet 22 s.

Riihimäki
Degree Programme in Information technology
Telecommunications technology

Author	Tommi Bäckman	Year 2013
Subject of Bachelor's thesis	Network devices' configuration management in Corenet Oy	

ABSTRACT

Corenet Oy is a small Finnish operator and integrator that offers special network solutions to its customers. Corenet Oy manages thousands of its own and its customers' network devices.

The purpose of this thesis was to find a suitable solution for a new configuration management tool for Corenet Oy. The tool should provide the means to perform, for example automated building, checking and backup of configuration files. The tool should also be able to handle mass configurations.

The work on the thesis started by making a survey for Corenet's specialists. The survey was made with Microsoft Sharepoint. The survey was directed to all workers who would be using the new tool. In addition to the answers, also invaluable comments were given, which were taken into consideration during the work on the thesis.

The requirement specification was formed based on the survey. A tender process between available solutions was started using the requirement specification and a scoring system defined in this thesis. The purpose of the tendering was to choose the most suitable tool for Corenet, either from available commercial or open source tools.

As a source of information, the Internet was invaluable but also interviews, books and training sessions were used as information sources. Naturally information from the different vendors also proved valuable.

The thesis was completed to a point where Corenet can make a selection from suitable configuration management tools. The final selection is not addressed in this work, but completed internally at Corenet.

Keywords Configuration, Network, Management, Open Source

Pages 32 p. + appendices 22 p.

SISÄLLYS

LYHENTEET	1
TERMIT	2
1 JOHDANTO.....	1
2 KONFIGURAATIONHALLINTA	3
2.1 Mitä konfiguraationhallinnalla tarkoitetaan?	3
2.1.1 Konfiguraationhallinta ja elinkaari	4
2.1.2 Dokumentointi ja konfiguraationhallinta	6
2.2 FCAPS-malli	7
2.3 Riskien ja ongelmatilanteiden hallinta konfiguraationhallinnan avulla.....	8
2.4 Konfiguraationhallinnan työkalut	10
2.4.1 Avoimen lähdekoodin (Open Source) ohjelmistot ja työkalut	10
2.4.2 Kaupalliset vaihtoehdot	11
2.5 Ennen ja nyt - mitä tulevaisuus voi tuoda mukanaan?	11
3 KONFIGURAATIONHALLINTA CORENETILLA	13
4 VAATIMUSMÄÄRITTELY	13
4.1 Kysely.....	15
4.2 Tulosten keruu ja analysointi	15
5 VAATIMUSMÄÄRITTELYSTÄ VALINTAKRITEEREIHIN	17
5.1 Tieto- ja tarjouspyyntö	17
5.1.1 Tietopyyntö - RFI	17
5.1.2 Tarjouspyyntö - RFP	17
6 VAIHTOEHDOT JA KILPAILUTTAMINEN	19
7 PISTEYTYYS JA VERTAILU.....	20
7.1 Pisteytysmenetelmä.....	20
7.2 Osallistujien vertailu	21
7.3 Lopullinen yhteenvedo.....	23
8 POC (PROOF OF CONCEPT)	25
9 ELINKAARIHALLINTA	26
10 LOPPUSANAT	29
LÄHTEET	30
HAASTATTELUT	31
LIITTEET	32

Liite 1	Requirement Specification
Liite 2	Opinnäytetyön kysely ja vastausten analysointi

LYHENTEET

ACL	Access Control List
BYOD	Bring Your Own Device
B2B	Business-to-business
B2C	Business-to-consumer
CMDB	Configuration Management Database
CoS	Class of Service
DB	Database
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
EOL	End-of-Life
EOS	End-of-Sales
FCAPS	Fault, Configuration, Accounting, Performance, Security
GPL	General Public License
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
LAN	Local Area Network
MAC	Media Access Control
OSI	Open Systems Interconnection Reference Model

PING Packet Inter-Networking Groper

POC Proof of Concept

QoS Quality of Service

RFC Request for Comments

RFI Request for Information

RFP Request for Proposals

ROI Return of Investment

SDN Software-defined Networking

SNMP Simple Network Management Protocol

SSH Secure Shell

WLAN Wireless Local Area Network

WLC Wireless LAN Controller

WWW World Wide Web

TERMIT

BYOD Bring Your Own Device. Käyttäjät tuovat omia päätelaitteitaan työpaikalle käyttäen niitä työnsä hoitoon.

Cloud Pilvi

Cloud Services Pilvipalvelut

Data Center Palvelinkeskus

Openflow Avoin standardi, joka sallii kokeellisten protokollien ajamisen esimerkiksi kampus-verkoissa

Private Cloud Pilvi-infrastrukturi, joka on sisäisesti tai kolmannen osapuolen kautta tietyn organisaation käytössä

Public Cloud Pilvipalvelu, joka toimii julkisen verkon yli ja on julkisessa käytössä

Sflow Protokolla, jolla valvotaan langallisen ja langattoman verkon ja palvelimien toimintaa

1 JOHDANTO

Konfiguraationhallinta on oppi kehittyvien järjestelmien organisoinnista ja hallinnasta. Konfiguraationhallinta pyrkii määrittämään menettelytavat komponenttien ja niiden yhdistelmien tunnistamiseksi, julkistusten ja muutosten hallitsemiseksi, tuotteen tilan kirjaamiseksi, sekä tuotteen täydellisyyden ja yhtenäisyyden varmistamiseksi. Tässä komponenteilla tarkoitetaan ohjelmistoalkioita, joita ovat muun muassa ohjelmatiedostot ja dokumentit. (Wikipedia n.d.)

Konfiguraationhallinta on erittäin tärkeää, koska ilman sitä, isompia verkkoja olisi lähes mahdotonta ylläpitää. Konfiguraationhallinta koostuu dokumenteista, tietokannoista, laitteiden konfiguraatietiedoista ja muista vastaavista tiedoista, ominaisuuksista ja järjestelmistä, joiden avulla verkon ylläpito helpottuu huomattavasti. Verkon ja verkkolaitteiden hallinnoiminen ilman soveltuvaa konfiguraationhallintaa on lähes ylivoimaisen vaikeaa. Dokumentaatioon sisältyvät muun muassa verkkolaitteiden IP-osoitteet, joita ilman laitteisiin on hyvin työlästä, ottaa etäyhteys.

Konfiguraationhallinnan automatisointi on haluttu ja käytetty toiminto nykyaikaisessa verkossa ja sillä pystytään tehokkaasti hallinnoimaan suuriakin määriä verkkolaitteita. Konfiguraationhallinnan työkaluja käyttäen on helppoa suorittaa jopa tuhansien laitteiden massakonfiguraatioita, konfiguraatioiden tarkistuksia ja varmuuskopioiden talteenottoa. Konfiguraationhallinta kattaa myös konfiguraatiomuutoksen havaitsemisen, konfiguraatioiden arkistoinnin, verkkolaitteiden dokumentoinnin ja verkkolaitteiden ohjelmistojen hallinnan.

Opinnäytetyö on tehty Corenet Oy:lle ja sen tarpeisiin. Corenet on pieni suomalainen operaattori ja integraattori, joka on erikoistunut toteuttamaan asiakkailleen tietoliikenteen erikoisratkaisuja. Corenet on VR-Yhtymä Oy:n ja TDC Oy:n yhteisyritys, joka on perustettu vuonna 1998. Corenetissä työskentelee noin 200 työntekijää, joista suurin osa työskentelee tietoliikenneverkkojen asiantuntijatehtävissä. Lisätiedot yrityksestä osoitteessa <http://www.corenet.fi>.

Corenet pyrkii olemaan valmistaja- ja laitteistoriippumaton. Toisin sanoen Corenetin tarjoamissa palveluissa ja tuotteissa hyödynnetään useiden erilaisten valmistajien laitteistoja. Valittavan työkalun tulee tukea sekä Corenetin että Corenetin asiakkaiden yleisesti käyttämiä laitteita. Laitteiden konfiguraatio-osuus voitaisiin esimerkiksi toteuttaa konfiguraatiopohjilla ("template"), luomalla tietokanta, jossa on erilaisia valmiita pohjia, joista parhaiten soveltuva valitaan tarpeen mukaan siirrettäväksi verkkolaitteelle.

Tässä työssä keskitytään asettamaan vaatimukset konfiguraationhallintatyökalulle ja tutkimaan erilaisia saatavilla olevia työkaluja ja vertailemaan näitä keskenään. Tarkoituksena on valita paras mahdollinen vaihtoehto, joka kattaa sille tässä työssä asetettavat vaatimukset.

Työn tavoitteena on löytää Corenetille työkalu, joka on hyvin skaalautuva, muokattava ja helppokäyttöinen. Eräs tutkittava vaihtoehto on avoimeen lähdekoodiin (Open Source) pohjautuva työkalut, joka kattaisi suurimman osan jo asetetuista vaatimuksista ja jota olisi helppo laajentaa täyttämään loputkin tarpeet lisämoduuleilla tai suoraan lähdekoodia muokkaamalla. Open Source-pohjainen työkalu ei kuitenkaan ole ainoa vartenotettava ratkaisu, vaan työssä huomioidaan myös tarjolla olevia valmiita kaupallisia vaihtoehtoja.

Työn alkuvaiheessa suoritetaan työkalun tuleville loppukäyttäjille kysely, jonka avulla luodaan tarvemäärittely. Tarvemäärittely osaltaan toimii pohjana määriteltäessä pisteytysjärjestelmää, jota hyödynnetään itse työkalun valinnassa, esimerkiksi kilpailutusvaiheessa tai suorahankintatilanteessa.

Työssä valitaan muutama potentiaalinen työkalun tarjoaja, joille lähetetään tarjouspyyntö. Tarjoajat esittävät kiinnostuksensa vastaamalla tarjouspyyntöön ja pääsevät siten mukaan kilpailutukseen, mikäli kaikki vaaditut vaatimusmäärittelyn osiot täyttyvät. Kilpailutus ja pisteytys tapahtuvat ennalta määrättyjä kriteerejä käyttäen. Kriteerit osaltaan pohjautuvat tarvemäärittelyyn.

Työn loppuvaiheessa esitetään ohjelmiston valintaperusteita perustuen vaatimusten täyttymiseen ja esitettyyn pisteytykseen. Valintaperusteiden paikansapitävyys tulee verifioida kenttätestein ennen lopullista valintaa ja käyttöönottoa. Lopullista valintaa tai kenttätestausta ei tässä opinnäytetyössä käsitellä syvällisemmin, vaan ne jäävät työn ulkopuolelle.

2 KONFIGURAATIONHALLINTA

Yleisesti uskotaan, että konfiguraationhallinnalla tarkoitetaan ainoastaan verkkolaitteiden konfiguraatitiedostojen hallintaa, mutta oikeastaan konfiguraatitiedostojen hallinta on vain pieni osa kokonaisuutta - eli osa tietoliikenneverkon hallintaa. Konfiguraationhallinta itsessään on kuitenkin (tietoliikenne)verkon hallintaan liittyvä laajahko osa-alue.

Laitekonfiguraatio määrittelee, miten verkkolaite toimii, joten se on itsessään todella tärkeä. Ilman oikeanlaista konfiguraatiota laitteen sekä mahdollisesti koko tietoliikenneverkon toiminta on vääränlainen. Pahimmassa tapauksessa vääränlainen konfiguraatio lamaannuttaa koko verkon toiminnan. Vain laitteen konfiguraatioon määritellyt ominaisuudet ovat käytössä ja muut toiminnallisuudet jäävät käyttämättä. Konfiguraationhallinnalla halutaan varmistaa, että oikeat, tarvittavat ominaisuudet ovat käytettävissä koko tietoliikenneverkossa, ja että verkko palvelee käyttötarkoitustaan mahdollisimman tehokkaasti ja virheettömästi.

2.1 Mitä konfiguraationhallinnalla tarkoitetaan?

Tässä työssä konfiguraationhallinnalla tarkoitetaan lähiverkkolaitteiden, kuten lähiverkkokytinten ja -reitittimien konfiguraatioita sekä niissä tapahtuvien muutoksien hallinnoimista ja seuranta. Konfiguraationhallinta toimii verkon hallinnan ja verkon elinkaaren kulmakivenä. Konfiguraationhallinnan avulla tiedetään, mitä laitteita verkossa on, ja lisäksi mahdollistetaan myös verkkolaitteiden hallinnointi. Hallinnan avulla voidaan myös varmistua siitä, että kaikki laitteet ovat konfiguroitu oikein ja että koko verkossa on samat säädöt ja säännöt. Esimerkiksi varmistetaan, että laatu-luokittelut, CoS (Class of Service) ja QoS (Quality of Service), toimivat samalla tavalla koko verkossa, että sovellusten aiheuttama liikenne sujuu mahdollisimman virheettömästi, ja että virheiden tapahtuessa verkko toipuisi nopeasti ja automaattisesti.

Konfiguraationhallinnan merkitys tulee vain kasvamaan jatkossa – siitä pitävät huolen jatkuvasti kasvavat liikennöintinopeudet ja erilaiset, muuttuvat, liikennöintitarpeet, sekä ennen kaikkea SDN-verkkojen (Software Defined Networks) tuleminen. SDN-verkoissa käytettävä sovellus määrittelee koko verkolle asetukset kohdilleen kulkemansa reitin osalta. Esimerkiksi palvelinkeskukset ja niistä tarjottavien sovellusten jakelu tulee mitä ilmeisemmin jatkossa rakentumaan pitkälti tämän tekniikan päälle. (Alcatel-Lucent, Satumäki, Koulutusmateriaali, 2013). SDN-verkkojen osalta on huomattava, että verkkojen rakenne muuttuu hyvin paljon litteämmäksi ("Flat") nykyisistä puumallisista verkoista. Verkkojen hallinnointi on entistä tärkeämpää ja haastavampaa uudistuvan verkkorakenteen myötä. Syynä tähän muutokseen on se, että liikenne ei enää kulje koneelta palvelimelle (host-to-host) vaan enemmänkin koneelta palvelinkeskukseen (host-to-cloud).

Lisäksi sflow ja openflow-protokollat tulevat ilmeisesti nousemaan tärkeiksi palvelinkeskustoiminnassa, jolloin protokollien toimivuus tulee varmistaa oikeanlaisilla konfiguraatioilla, jotta taataan verkon ja ennen kaikkea sovellusten toimivuus. Luonnollisesti tämä vaatii myös laitteiden yhteensopivuutta sekä tuen käytettäville protokollille.

2.1.1 Konfiguraationhallinta ja elinkaari

Konfiguraationhallinnalla yhdistetään tietoliikenneverkon elinkaaren eri vaiheet toisiinsa. Tietoliikenneverkon elinkaaren eri vaihteita ovat esimerkiksi:

- valmistelu
- ennakkosuunnittelu
- verkkosuunnittelu
- toteutus
- toiminta
- optimointi.

(Cisco Systems, 2007, 4)

Luonnollisesti kaikilla tietoliikenneverkon laitteilla ja osilla on myös oma elinkaarensa, esimerkiksi komponenttien elinikä. Lisäksi myös laitteen sisällä olevalla käyttöjärjestelmällä, sekä luonnollisesti käyttöjärjestelmän toimintamäärittelyllä, konfiguraatiolla, on oma elinikänsä. Elinkaari liittyy tietoliikenneverkon koko toimintaan ja tulee huomioida projekteissa, joiden myötä verkko kasvaa ajan myötä.

Verkkoprojekteiksi määritellään kaikki tietoliikenneverkkoon liittyvät hankkeet, jotka vaativat suunnittelua. Kaikkien suunnitelmien on mahdollista ennalta suunniteltuun ja hyväksytyyn verkkoarkkitehtuuriin. Verkoarkkitehtuuri on päivitettävä, kun tietoliikenneverkolle esimerkiksi asetetaan uusia vaatimuksia. Yleensä verkkoarkkitehtuuri määritellään jo suunniteltaessa tietoliikenneverkkoa. Verkoarkkitehtuuri jää usein päivittämättä, vaikka verkolle asetetaan uusia, arkkitehtuuriin vaikuttavia, vaatimuksia.

Ohjelmistopäivitys pidentää myös laitteiston elinkaarta, sillä se tuo usein uusia ominaisuuksia, korjaa ohjelmistovirheitä ohjelmistosta tai paikkaa tietoturva-aukkoja. Päivitettäessä on pidettävä huoli uusista ominaisuuksista ja mahdollisesta konfiguraatiosyntaksin muuttumisesta. Tiedostorakenteet tai tiedostot voivat muuttua päivityksessä, mikä on huomioitava, jotta laitteen toiminta turvataan. Siirryttäessä uuden ohjelmistoversion käyttöön on valmistelut ja testaukset tehtävä huolellisesti sekä on luotava palautussuunnitelma. Päivitykset ja testaukset, erityisesti palautussuunnitelman testaus, olisi hyvä toteuttaa erillisessä laboratorioverkossa ennen kuin tehdään vastaavat muutokset tuotantoverkkoon.

Tietoturva tulee ottaa huomioon myös verkkoja suunniteltaessa – riskien muodossa, ellei muuten. Äärimmilleen vietynä voi tietoturvariskien takia olla täysin erilliset verkot kriisitoimintaa ja tavallisia tuotantotoimia varten, kuten esimerkiksi Suomen Puolustusvoimilla.

Kaikki verkon muutokset, jotka eivät vaadi verkkoarkkitehtuuriin vaikuttavaa suunnittelua, mukaan lukien tuotantoympäristön optimointi, ovat toiminnallisia muutoksia. (Cisco Systems, 2007, 4).

Yleisellä tasolla voidaan vaiheiden lisäksi tunnistaa eri rooleja tietoliikenneverkon toimittamisessa ja tukemisessa:

- projektin hallinta (management)

- verkon arkkitehtuuri (architecture)
- toimitus (delivery) (laitteet, asennus ja konfigurointi)
- tuki (support) (laite- sekä konfiguraatiotuki, mahdollisesti sovellustuki-kin)
- valvonta (laite, yhteydet, laitehyvinvointi) katsotaan tässä sisältyvän tukirooliin.

Taulukossa 1 on lueteltu erilaisia toiminteita sekä roolit joiden vastuulla toiminnot ovat. Tämän tyyppinen vastuujako voidaan hyödyntää jopa yrittäjäyrityksissä.

Taulukko 1. Eri vastuualueiden roolit.

	Hallinta	Arkkitehtuuri	Toimitus	Tuki ja valvonta
Valmistelu	X	X		
Ennakkosuunnittelu	X	X		X
Verkkosuunnittelu		X	X	X
Implementointi			X	X
Toiminnallisuus		X		X
Optimointi		X		X

Konfiguraatiohallinta ei silti ole pelkästään verkkolaitteiden tietojen keräämistä ja konfigurointia, vaan se sisältää myös ne prosessit, joita tarvitaan verkon ylläpitoon, tukemiseen ja toimintaan liittyen. Itse verkonvalvonta ei kuulu konfiguraatiohallintaan, vaan on oma kokonaisuutensa.

Konfiguraatiohallintaan voidaan sisällyttää seuraavat asiat:

- laitteiden laitteisto- ja ohjelmistotietojen kerääminen
- laitteiden ohjelmiston hallinta
- laitteiden konfiguraation varmuuskopiointi, katselu, arkistointi ja vertailu
- muutoksien havainnointi ja laitteen konfiguraatio-, laitteisto- tai ohjelmistomuutoksista hälyttäminen
- konfiguraatiomuutosten täytäntöönpano

(Cisco Systems, 2007, 2)

Verkot muuttuvat jatkuvasti ja lisäksi muutosnopeus on viime vuosina kasvanut uusien käytötapojen ja sovellusten vallatessa tilaa, eli yhä useampia muutoksia tulee huomioda verkoissa yhä nopeammalla syklillä. Esimerkkejä tällaisista muutoksista on voimakkaasti kasvava määrä langattomia laitteita. Usein laitteet ovat jopa käyttäjien omia (BYOD – Bring Your Own

Device). Myös yhä useampia palveluita käytetään niin sanottuina pilvipalveluina joko julkisista palvelinkeskuksista tai yrityskohtaisista palvelukeskuksista (private cloud). Pilvipalvelut asettavat monesti myös vaatimuksia lähiverkon toiminnalle ja siten konfiguraatioille.

Konfiguraationhallinta on tarkoitettu helpottamaan erityisesti suurien ja laajojen verkkojen hallintaa. Erityisen tärkeää verkkojen hallinta on silloin, kun on kyse operaattoreista, integraattoreista tai palveluntarjoajista, jotka hallinnoivat ja toteuttavat jopa tuhansien asiakkaiden tietoliikenneverkkoja. Tästä syystä kaikenlainen automaatio on tärkeää ja se myös auttaa välttämään inhimillisten virheiden tapahtumista, joita voi tapahtua esimerkiksi yhden asiantuntijan vastatessa useasta asiakasverkosta. Tällä tähdätään myös siihen, että säästyisi aikaa, ja että perustoimet voidaan automatisoida esimerkiksi asiantuntijoiden suunnitelmia seuraten.

2.1.2 Dokumentointi ja konfiguraationhallinta

Dokumentointi on erittäin tärkeää tuotantoympäristössä. Siitä selviää verkon staattinen tila tietyllä ajanhetkellä – staattisuus on samalla myös suuri heikkous. Staattisen dokumentaation käyttöikä on hyvin lyhyt dynaamisessa verkossa, koska dokumentaatiota on muutettava jokaisen verkkoon tehdyn muutoksen myötä. Toisaalta staattisessa verkkoympäristössä dokumentaation käyttöikä voi olla useita vuosia. Staattisia verkkoja löytyy nykyään lähinnä tuotantolaitoksista ja tehtaista. Näissäkin staattisen verkot muuttuvat hiljalleen esimerkiksi sähköisen tuotannonohjauksen käyttöön-oton myötä.

Nykyaikaiset yritysverkot kehittyvät SDN-verkkojen suuntaan, jolloin jopa verkon muutokset ja asetukset voivat tulla palveluntarjoajalta tai muokkaantua käytettävän sovelluksen mukaan (pilvisovellus). Tämäntapaiset muutokset voivat johtaa kaaokseen ellei ole olemassa menetelmiä, joilla muutokset dokumentoidaan ja palautetaan ennalleen esimerkiksi käyttäjän lopettaessa sovelluksen käytön. Ellei SDN-verkko kykene tällöin palauttamaan tilannetta ennalleen tulee konfiguraatio olla palautettavissa konfiguraationhallintajärjestelmän avulla. SDN:ssä käytettäviä protokollia ei ole vielä määriteltä tai saatu standardisoitua, mikä tarkoittaa, että tilanne tulee olemaan erittäin haasteellinen yhteensopivuuden osalta.

Dokumenttien muutoshistoria on hyvä tarkistaa, mikäli epäillään jonkin verkkoon tehdyn muutoksen aiheuttaneen toimimattomuutta. Asiantuntija voi kirjoittaa, mitä on tehty ja milloin, jolloin seuraava työstäjä saa ensikäden tietoa asiasta. Dokumenteista pitää käydä ilmi muutokset ja päivitystiedot, jotka on myös pidettävä ajan tasalla. Dokumentinhallintaa helpottaa monissa yrityksissä käytössä olevat dokumentinhallintajärjestelmät, joissa hyödynnetään muutos- ja versiohallintaa.

Verkkokuvat ovat myös päteviä dokumentointikeinoja, vaikka nekin ovat staattisia. Niistäkään ei heijastu verkon sen hetkinen tilanne, ellei niitä pidetä ajan tasalla. Verkonhallinnan puolella on toki järjestelmiä, joiden avulla voidaan automaattisesti piirtää verkkokuvia ja seurata muutoksia linkeissä ja reitityksissä. Näitä ei kuitenkaan käsitellä lähemmin tässä työssä.

Verkonhallintaohjelmistot eivät yleensä ota kantaa itse konfiguraatioihin, vaan seuraavat verkkomuutoksia ja laitteiden hyvinvointia. Useat tällaiset ohjelmistot osaavat antaa hetkittäisen kuva verkon tilasta tilannekuvana ("snapshot"). Snapshot voi sisältää verkkokuvia, laitetietoja ja tilatietoja, hälytystietoja ja niin edelleen, joiden avulla voidaan suorittaa esimerkiksi virheenkorjausta.

Kun asiantuntija selvittää verkkovikaa, on ensiarvoisen tärkeää, että dokumentaatio on ajan tasalla. Asiantuntijan on voitava luottaa dokumentaatioon ja siinä kuvatun tiedon on oltava relevanttia ja ajan tasalla.

Tehokkaalla konfiguraationhallinnalla, muutoshallinnalla ja muilla asianmukaisilla prosesseilla verkon valvonta ei koidu ylitsepääsemättömäksi haasteeksi. Prosessit voivat esimerkiksi seurata ITIL-määrittelyjä (Information Technology Infrastructure Library), mikäli kaivataan formaaleja prosesseja toiminnan tueksi. Luonnollisesti tarvitaan myös toimintaa tukevia organisaatorakenteita, jotta toiminta olisi tehokasta. Rakenteetkin voidaan toteuttaa ITIL:in määrittelyjen pohjalta tai vaikka seuraten aiemmin esiteltyä taulukkoa, (Taulukko 1).

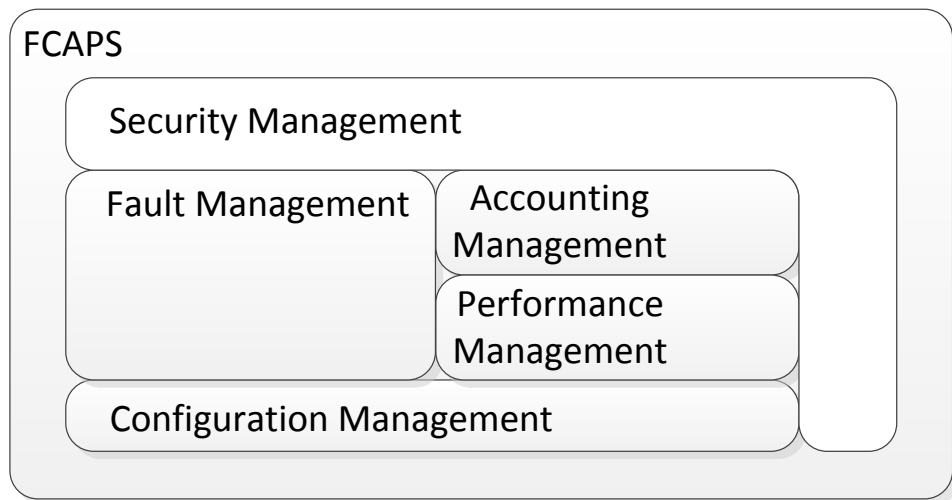
2.2 FCAPS-malli

Verkon hallinnalle, samoin kuin verkkokerroksille, on kehitetty kansainvälinen ISO-standardi (International Organization for Standardization). Verkon hallinnan ISO-standardi on nimeltään FCAPS. Malli toimii myös usein verkonhallinnan viitekehityksenä. FCAPS-mallin kirjaimet tarkoittavat seuraavaa:

- F, Fault management, vianhallinta
- C, Configuration management, konfiguraatiohallinta
- A, Accounting management, järjestelmätilien hallinta
- P, Performance management, suorituskyvyn hallinta
- S, Security management, tietoturvan hallinta

(Cisco Systems, 2007, 2)

Konfiguraation hallinta (Configuration Management) on C-kirjain FCAPS-mallissa. Konfiguraation hallinta on avaintekijä tässä mallissa, vaikka usein ajatellaan että jokainen osa-alue olisi tasavertainen. Kuvasta 1 käy paremmin ilmi miten tämä malli huomioi tietoliikenneverkon hallinnan eri osa-alueet.



Kuva 1. Verkonhallinnan FCAPS-malli ja eri osa-alueet.

Kuten kuvasta käy ilmi, rakentuvat mallin muut osa-alueet konfiguraatiohallinnan päälle.

2.3 Riskien ja ongelmatilanteiden hallinta konfiguraationhallinnan avulla

”Riskienhallinta on seurauksiltaan merkittävien kielteisten tapahtumien (riskien) järjestelmällistä määrittelyä ja niihin varautumista” (Wikipedia, 2013).

Tietoliikenneverkossa on tärkeää varautua kaikenlaisiin riskeihin, koska pienikin virhe voi lamaannuttaa koko verkon. Jos riskeihin varaudutaan ennakoon ja luodaan palautussuunnitelmat, tai konfiguraationhallinta otetaan mukaan prosessiin, niin virheistä toipuminen on nopeampaa ja vaivattomampaa kuin ilman palautussuunnitelmaa ja konfiguraatiohallintaa. Riskienhallinta kannattaa sisällyttää konfiguraationhallintaan, koska konfiguraatiohallinnalla voidaan estää tai korjata monia virheitä tai ongelmia oikein toteutettuna.

Ward Hollowayn (2012) mukaan konfiguraationhallinta itsessään on riskienhallintaa. Esimerkiksi, jos reitittimen ylläpitäjä lisää laitteelle pääsylvästan (ACL - Access Control List), joka sallii pääsyn ulkoverkosta sisäverkkoon, niin se on suuri riski koko verkolle. Samoin käy jos palomuurin ylläpitäjä sallii vahingossa kyseisen liikenteen ulkoverkosta sisäverkkoon. Holloway painottaa, että tällaisiin riskeihin ja tapahtumiin tulisi kiinnittää erityistä huomiota. Konfiguraationhallinta pitäisikin siksi sisällyttää päivittäiseen riskienhallintaan ja tietoverkkotoimintaan, sillä sen avulla voidaan saada hälytys kuvatus muutoksen tapahtuessa laitteella.

Alla on lueteltu muutamia esimerkkejä, miten konfiguraationhallinnalla voidaan vaikuttaa riskeihin.

- Muutoksen suorittaja ei ole paikalla, jos jotain tapahtuu hänen tekemänsä muutoksen myötä. Kenelläkään muulla ole tiedossa, mitä kyseinen henkilö on tehnyt. Ongelman aiheuttanutta muutosta on tällöin usein vaikea etsiä ja

korjata. Toinen vaihtoehto on, että tuotantoverkkoon on tehty konfiguraatiomuutoksia, jotka eivät näy hallinnassa.

Riskien välttämiseksi, ja jotta vikatilanteissa pystyttäisiin toimimaan tehokkaasti, on dokumentaatio, muutosseuranta ja tiedot tekijästä oltava kunnossa. Kun nämä on kunnossa, on edellä mainitut tilanteet helpompi korjata.

- Hälytykset kertovat, mikä laite on mennyt rikki tai on sähköittä, mutta vian paikallistaminen, laajuuden arviointi ja mahdollisten muiden riskien analysointi manuaalisesti vie paljon aikaa - puhumattakaan viankorjauksen viivästymisestä.

Verkkokuvat, seuranta-Excelit ja toimipistelistaat ovat tärkeässä asemassa, jotta voidaan nähdä esimerkiksi jonkin tietyn toimipisteen verkkotopologia yhdellä silmäyksellä. Hyvin tehty topologiakuva kertoo lähes välittömästi, millä laajuudella vikaa mahdollisesti esiintyy ja mitä muita riski- tai virhetekijöitä on havaittavissa.

- Verkko ei kykene palauttamaan konfiguraatioita normaalitilaan (SDN)

Välillä voi käydä niin, ettei verkko kykene palautumaan vikatilanteista tai palauttamaan konfiguraatioita normaalitilaan, jolloin on kätevää olla olemassa jokin konfiguraation automaattipalautuksen kaltainen toiminne, joka lataa palvelimelta uusimman toimivan konfiguraation ja ajaa sen laitteelle havaittuaan, ettei kaikki ole kunnossa. Tällöin palautusprosessin laukaisu-tekijöiden on oltava kunnossa ja toiminnassa.

- Ohjelmistopäivitys sekoittaa konfiguraatiot

Ohjelmistopäivityksestä johtuvat vikatilanteet voisi myös selvittää edellisen kaltaisella menetelmällä, jolloin ohjelmiston versio tarkistetaan jokaiselta laitteelta. Verkon hallittavuuden kannalta on hyvä pyrkiä yhtenäistämään ohjelmiston versiot toimivaksi todettuun versioon koko verkossa. Tällä taataan lisäksi se, että kaikki ominaisuudet ovat käytettävissä koko verkossa. Lisäksi pyritään usein myös verkkolaitteiden yhdenmukaisuuteen eli samassa verkossa pyritään pidättäytymään muutamassa laitemallissa ylläpidollisista syistä.

- Verkkohyökkäys sekoittaa konfiguraatiot tai niitä joudutaan muuttamaan sen takia.

Verkkohyökkäyksen, tietomurron tai verkkolaitteiden ryöstön tapahtuessa tulisi koko verkko konfiguroida uudelleen tietoturvasyistä. IP-osoitteet tai vähintään kirjautumistiedot on hyvä vaihtaa koko verkkoon. Tässä asiassa konfiguraationhallinnan massakonfigurointiominaisuus pääsee oikeuksiinsa. Järjestelmään syötetään konfiguroitavien laitteiden tiedot ja kerrotaan, mitä konfiguraatioon muutetaan. Tämän jälkeen järjestelmä ajaa halutut tiedot jokaiseen verkkolaitteeseen. Parhaassa tapauksessa tämä toiminne myös tuhoaisi vanhat konfiguraatiot, jolloin niitä ei voisi vahingossa joutua laitteille. Tuhottujen konfiguraatioiden tilalle tulisi tällöin tallettaa ensimmäinen versio uudesta konfiguraatiotiedostosta.

Mike Rothmanin (2012) mukaan konfiguraatiohallinnan tukena voidaan esimerkiksi käyttää myös erilaisia skannereita, jotka luotaavat koko ajan koko verkkotopologiaa ja ilmoittavat viallisista kohdista konfiguraatioissa ja verkossa. Kyseiset skannerit myös ilmoittavat haittaohjelmista ja muista haavoittuvuuksista verkossa ja lisäävät näin ollen tietoturvaa. Securosis on kertonut näistä skannereista ja niiden integroitavuudesta konfiguraationhallintaan ja versionhallintaan blogissaan (<https://securosis.com/blog/the-pragmatic-guide-to-network-security-management-the-process>).

2.4 Konfiguraationhallinnan työkalut

Konfiguraationhallintaa ja riskienhallintaa helpottamaan on saatavilla useita erilaisia työkaluja, jotka voidaan karkeasti jakaa kahteen ryhmään; avoimen lähdekoodin työkaluihin ja kaupallisiin ohjelmistoihin. Lisäksi on tarjolla muutamia ohjelmistoja, jotka ovat näiden kahden sekoitus, jolloin tietty osa ohjelmistosta on kaupallinen ja osa kehitetty avoimen lähdekoodin alla. Nämä lasketaan tässä työssä kaupallisiksi ohjelmistoiksi.

Valmistajat ovat huomanneet markkinaraon ja tarjoavat nykyään monenlaisia hallintatyökaluja. Jotkut työkalut koostuvat osista, moduuleista, joita myydään erillisinä osina. Toiset työkalut taas sisältävät kaikki samat toiminnallisuudet yhdessä paketissa. Lisäksi monet työkalut sisältävät hallinta- ja valvontatyökaluja samassa, tai joitakin konfiguraatiohallintaominaisuuksia on sisällytetty valvonta- ja hallintasovelluksiin.

Työn aikana tuli huomattua myös se, miten paljon yritykset antavat ilmaiseksi tiettyjä moduuleja jouduttaakseen lisämoduulien myyntiä. Jotkin yritykset taas myyvät tuotteitaan mahdollisimman halvalla taatakseen mekin.

2.4.1 Avoimen lähdekoodin (Open Source) ohjelmistot ja työkalut

Avoimen lähdekoodin työkalut ovat usein hankittavissa ilmaiseksi tai pienin kustannuksin ja niitä voi melko vapaasti kehittää eteenpäin parhaaksi katsomaansa suuntaan. Kehitysmahdollisuudet riippuvat siitä, minkä avoimen lähdekoodin lisenssin alla työkalu on julkaistu, esimerkiksi OpenGPL, GPL, GNU GPL. Joissain tapauksissa muutokset on pakko julkistaa – joissain tapauksissa kehitystä saa suorittaa vapaasti. Tarkoituksena on, jos mahdollista, etsiä vaihtoehto, jossa tehtyjä muutoksia ei tarvitse julkaista kaikkien saataville.

Avoimen lähdekoodin puolella on kaksi pääsuuntaa; ohjelmistot, joita kehittävät alan harrastajat tai osaajat erilaisissa yhteisöissä, ja sitten ne, joissa on mukana jokin formaali taho, yleensä yritys, johtamassa kehitystä. Toisena mainitussa tapauksessa yrityksellä voi olla omia kehittäjiä tai samat harrastajat tekevät kehitystä, mutta formaali taho päättää, mitä julkaistaan ja milloin. Usein nämä tahot tarjoavat lisäksi ohjelmistotukea itse ohjelmiston rinnalla. Esimerkkeinä toimivat RedHat/Fedora, Ubuntu ja näiden tuottamat Linux-versiot.

Näitä vaihtoehtoja ei kuitenkaan voi suoraan verrata kaupallisiin vaihtoehtoihin, joiden kehittämisen lähtökohdat ovat yleensä hyvinkin erilaiset niin tekniseltä osalta kuin ajatusmalliltaan. Suurten verkkojen hallintatyökalun kehittäminen vaatii pääsyä laajaan skaalaan verkkolaitteita, johon avoimen lähdekoodin kehittäjillä hyvin harvoin on mahdollisuutta.

Nämä vaihtoehdot ovat kuitenkin siinä mielessä etulyöntiasemassa, että ne tarjoavat laajan tuen eri laitevalmistajille, eivätkä keskity vain yhteen valmistajaan, kuten kaupalliset vaihtoehdot yleensä. Lisäksi uusia ominaisuuksia pystytään kehittämään nopeasti vastaamaan käyttäjien tarpeita maailmanlaajuisesti.

Hyvinä esimerkkeinä avoimen lähdekoodin järjestelmistä toimivat DeviceExpert, Rancid, Puppet Labs ja opConfig. Näillä työkaluilla yritys voi rakentaa jo lähes täydellisen konfiguraationhallinnan, koska ne ovat monipuolisia, kattavia ja laajennettavissa tarpeen vaatiessa.

2.4.2 Kaupalliset vaihtoehdot

Monet valmistajat tarjoavat kaupallisia vaihtoehtoja konfiguraatioiden hallintaan, mutta nämä työkalut ovat usein keskittyneet tietyn laitevalmistajan laitteiden hallintaan tai ovat osa jotain laajempaa kokonaisuutta. Monesti nämä kaupalliset vaihtoehdot ovat lisäksi suunniteltu lähinnä sovellusten hallintaan, kuten muutosten suorittamiseen erilaisille palvelimille, esimerkiksi Apache- ja SQL-palvelimille. Esimerkkejä kaupallisista työkaluista ovat IBM:n Tivoli Netcool -tuoteperheen Configuration Management Tool, Hewlett-Packard:n Encore, Cisco Systemsin CiscoWorks ja Alcatel-Lucen- tin OmniVista.

Eroja on lisäksi yritys- ja operaattorityökalujen välillä. Operaattoreille on tarjolla erilaisia ja varsin hinnakkaita työkaluja. Työkalut ovat kuitenkin monesti suunnattu operaattoriverkon hallintaan ja ylläpitoon, kuten b2c- (Business-To-Consumer) ja b2b (Business-To-Business)-verkkoihin eivätkä ole niinkään suunniteltu asiakaslähiverkkojen (LAN) tai langattomien lähiverkkojen (WLAN) hallintaan ja ylläpitoon. Joitain kuluttajasegmentin laitteistoja kyetään kyllä hallinnoimaan ja konfiguroimaan näillä työkaluilla, mutta se on valmistajakohtaista eikä kuluttajalaitteita pääsääntöisesti käytetä yritysverkoissa. Käyttötarkoitus huomioitaessa tällaiset työkalut eivät suoraan sovellu Corenetin käyttöön.

2.5 Ennen ja nyt - mitä tulevaisuus voi tuoda mukanaan?

Materiaalia kerätessä opinnäytetyötä varten löydettiin Susan Dartin (1992) kirjoittama ja Yhdysvaltojen puolustusvoimien rahoittama, tutkielma.

Tutkielmassa perehdytään siihen, mitä haasteita konfiguraationhallinnassa oli ollut, oli tuolloin ja mitä haasteita tulevaisuus toisi tullessaan. Tekstissä mainitaan, että samat ongelmat ovat olleen läsnä jo 20 vuotta. Nyt 21 vuotta

myöhemmin voidaan tekstiä edelleenkin pitää ajantasaisena, sillä edelleen kamppaillaan juuri samojen ongelmien kanssa. Toisin sanoen verkkojen haasteet ovat olleet tiedossa jo yli 40 vuotta niiden pysyessä lähestulkoon samoina koko tuon ajan.

Dart listasi viisi pääaihetta, joiden uskoi tuovan haasteita tulevaisuudessa: teknologia, prosessien suuntautuminen, hallinta, poliittiset ongelmat ja standardointi. On helppo todeta, että nopea teknologinen kehitys ja muutos ovat tulleet jäädäkseen, eikä aineistossa ole luonnollisesti kyetty huomioidaan nykyisiä kehityssuuntia, kuten esimerkiksi openflow- ja SDN-verkkoja, jotka osaltaan tulevat jatkossa muokkaamaan verkkojen jokapäiväistä toimintaa aivan uuteen, ennen näkemättömään suuntaan.

Yleinen standardointijärjestelmä on yleensä aina jäljessä, joten on hyvin todennäköistä, että jatkossakin tullaan näkemään valmistajakohtaisia standardeja niin kuin tähänkin asti. Erityisen mielenkiintoista on, miten sovellukset tulevat vaatimaan standardikehitystä tai muita yhteensopivuusmäärittelyjä toimiakseen. Standardointi ja varsinkin valmistajien omat standardit lisäävät haastetta, koska laitteet eivät välttämättä ole keskenään yhteensopivia. Prosessipuolella taas IT-hallinto on keskittynyt lähestulkoon yksinomaan ITIL-prosesseihin, vaikka muitakin rakenteita ja malleja on olemassa.

Poliittisena ongelmana voidaan nähdä esimerkiksi intressien törmäminen ja standardien erilaisuus USA:n ja Euroopan välillä. Myös standardiorganisaatiot standardoivat lähes samoja protokollia ja menetelmiä (ISO, IETF, IEEE, ITU) ja kisaavat näin keskenään. Jokaisella maalla on lisäksi omat kehityshintressinsä ja lainsäädäntönsä, jotka vaikeuttavat poliittisen yksimielisyyden saavuttamista tietoliikenneasioissa. Lisäksi tietoliikenneverkkoja käytetään nykyään poliittisena painostuskeinona, erityisesti erilaisia verkko-ohjelmia ja haittaohjelmia, esimerkiksi Flame-, Stuxnet-haittaohjelmat ja Viron tietoliikenteen lamauttaminen, hyödynnetään poliittisina aseina. Poliittinen verkkopainostus on myös nopeasti suuri tietoturva-aste.

Osa tekstissä mainituista ongelmista koskee lähinnä yhteen liitettyjen tietoliikenneverkkojen (Internet) ongelmia tai suljettuja yritys- tai julkishallinnon verkkoja. Täysin erillisiä verkkoja ei juuri enää ole, joten mainitut ongelmat ovatkin pikemminkin siirtyneet koko tietoyhteiskunnan yhteisiksi ongelmiksi.

Kaikesta päätellen odotettavissa on, ettei tilanne muutu ainakaan helpommaksi tulevaisuudessa, vaan seuraavankin kahdenkymmenen vuoden jälkeen ongelmat ovat samoja, joskin ilmenevät eri tavoin kuin tällä hetkellä. Tämä siitä syystä, että kehitys on nopeutunut ja kilpailu markkinoilla on erittäin kovaa kaikkien valmistajien vetäessä vielä omaan suuntaansa kehittäessään ratkaisujaan.

3 KONFIGURAATIONHALLINTA CORENETILLA

Corenet dokumentoi tällä hetkellä jokaisen asiakkuuden, asiakkaan laitteet ja siirtoverkkoyhteydet kattavasti. Dokumentaatio koostuu muun muassa Excel-tiedostoista ja verkkotopologiakuvista sekä CMDB:hen (Configuration Management DataBase) talletetuista tiedoista. Dokumenteissa on versionhallintatoiminne, jonka avulla dokumentin muokkaaja ilmoittaa muille asiantuntijoille, mitä muutoksia hän teki kyseessä olevaan dokumenttiin. Muut pääsevät sitten katsomaan versiohallinnan kautta, milloin erimerkiksi jokin laite on lisätty verkkokuvaan tai poistettu sieltä.

Verkkolaitteiden konfiguraatiomuutokset hoidetaan tänä päivänä pääosin käsin, mutta varmuuskopiointi tapahtuu suurimmaksi osaksi automaattisesti. Varmuuskopiot siirretään automaattisesti tiedonkeruupalvelimelle (probe). Tiedonkeruupalvelin on asiakkaan verkkoon asennettava palvelin, jonka avulla asiakkaan verkosta kerätään tietoja laitteiden hyvinvoinnista ja laitteiden lähettämistä hälytysviesteistä. Hälytystiedot lähetetään edelleen keskitettyyn hälytysten käsittelyjärjestelmään, valvontajärjestelmään, jonka yhteydessä on tietopankki kaikista asiakkaiden verkkolaitteiden konfiguraatioista. Tiedonkeruupalvelimelta konfiguraatiotiedot siirretään keskitettyyn kantaan tietyin väliajoin pitkäaikaissäilytystä varten.

Corenet haluaa nyt muuttaa tilannetta siten, että konfiguraatiohallinta automatisoidaan soveltuvin osin, tarkoituksena säästää aikaa ja rahaa, antamalla asiantuntijoiden keskittyä vaativampiin tehtäviin. Konfiguraatiohallinnan työstämistä varten perustettiin oma hanke, jonka osana tämä opinnäytetyö toteutettiin. Hankkeeseen kuuluu vaatimusmäärittely, kilpailutus, järjestelmän valinta ja käyttöönotto. Opinnäytetyö kattaa näistä toiminnoista suurimman osan ja toimii siten tärkeässä roolissa hankkeessa.

4 VAATIMUSMÄÄRITTELY

Vaatimusmäärittelyn täytyy olla tavoitelähtöinen prosessi. Organisaation tavoitteet täytyy olla hyvin selvillä, jotta voidaan lähteä rakentamaan määrittelyjä. Vaatimukset itsessään määrittävät, miten uusi järjestelmä voi täyttää kaikki sille asetetut tehtävät. Vaatimukseen täytyy sisällyttää sellaisia tekijöitä, jotka työkalun on pakko täyttää, muuten se on ihan turha. Täytyy siis miettiä esteet, jolloin tavoitteisiin on mahdotonta päästä, ja rajoitteet, jotka mahdollistavat asetetut tavoitteet. Lisäksi vaatimusmäärittelyssä tulee esittää vaatimukset ja tavoitteet mahdollisimman selkeästi ja yksityiskohdallisesti. (Tiensuu, haastattelu 2013.)

Vaatimusmäärittelyä tehtäessä on vertailtu useita eri vaatimusmäärittelydokumenteja ja myös seurattu Corenetilla yleisesti käytettyä tapaa tehdä sovellus- ja ohjelmistohankintoja. Corenetissa käytetään suurimmaksi osaksi seuraavaa vaiheistusta hankinnoissa:

- 1) Määrittely
- 2) Kilpailutus

- 3) Vertailu ja valinta
- 4) Soveltuvuustestaus (POC – Proof Of Concept)
- 5) Lopullinen valinta
- 6) Käyttöönotto (rollout)

Käyttöönotto toteutetaan useimmiten omana projektinaan, jotta voidaan paremmin varmistaa onnistunut siirtyä ohjelmiston käyttöön.

Määrittely voi pitää sisällään erilaisia esimäärittelyjä tai työpajoja, joissa asiantuntijat rakentavat yhdessä määrittelyjä. Corenetinlla sekä tässä työssä käytettävä malli löytyy melkein sellaisenaan kirjallisuudesta, esimerkiksi Ikonen ja Kalliola, 1996, mainitsee samankaltaisen määrittelytyön, joka sisältää seuraavat osuudet:

- 1) Kysely
- 2) Tulosten keruu
- 3) Tulosten analysointi

Kyselyn tekeminen kuuluu niin sanottuihin perinteisiin menetelmiin vaatimusten selvittämisessä. Muita käytössä olleita perinteisiä menetelmiä olivat muun muassa aivoriihi, asiantuntijoiden haastattelut ja työryhmät. Näiden avulla rakennettiin toimiva kokonaisuus, jonka avulla selvitettiin työlle asetettavat vaatimukset.

(Itä-Suomen yliopisto 2007.)

Vaatimusmäärittely pitää sisällään kaiken sen, mitä asiakas haluaa tuotteen/järjestelmän tekevän. Määrittelyn tulee olla tarkka ja virheetön. Koko kehitystyön ja käyttöönoton tulee pystyä perustamaan siihen. On siis otettava huomioon ensisijaisesti loppukäyttäjien, tässä tietoliikenneverkon asiantuntijoiden, vaatimukset ja mielipiteet, saatavilla oleva teknologia ja sen rajoitteet (laitteet, ohjelmat, tuki) sekä käytettävissä olevan työpanoksen ja pääoman määrä.

Vaatimusmäärittelyä tehtäessä on oltava kärsivällinen, koska yleensä ensimmäinen määrittely ei ole lopullinen, vaan se hahmottuu pikkuhiljaa projektin edetessä. Vaatimukset myös usein muuttuvat matkan varrella, ja järjestelmän eri osille voi olla omat vaatimuksensa. On osattava myös kysyä oikeat kysymykset, jos halutaan vastauksia epäselviin kohtiin - asiat voivat olla tilaajan päässä selvillä, mutta ne ovat alitajuisia ja niitä pidetään itsensä selvyyksinä, eikä niitä tuoda välttämättä esille muutoin kuin kysyttäessä.

(Tiensuu, haastattelu 2013.)

Vaatimusmäärittely syntyi pitkälti edellä mainitun mukaisesti. Esitietojen pohjalta rakennettiin vaatimusmäärittelyn runko, jota tarkennettiin kyselyyn tulleiden vastausten perusteella. Lopullisen muodon vaatimusmäärittely sai työryhmän keskustelujen myötä. Vaatimusmäärittely itsessään on erillinen dokumentti, joka löytyy työn liitteestä 1.

4.1 Kysely

Corenetin asiantuntijoille tehtiin edellisessä kappaleessa esitettyä mallia seuraten kysely. Kyselyssä valittiin työryhmän 10 tärkeimmäksi kokemaa kysymystä ja lisättiin ”vapaa sana”-osio, jossa asiantuntijat saivat antaa palautetta sekä tuoda esiin omia näkemyksiään. Asiantuntijoille lähetetyn kyselyn kysymykset perustuivat kolmesta jäsenestä koostuneen työryhmän näkemykseen tarpeellisista tiedoista sekä nykyisten järjestelmien tunnistettuihin puutteisiin ja heikkouksiin.

Lisäksi kyselyä laadittaessa hyödynnettiin myös kognitiivista menettelytapaa, eli Corenetin asiantuntijoilta pyydettiin erikseen alustava lista työkalun halutuista ominaisuuksista. Kyseistä menettelytapaa kutsutaan tehtäväanalyysiksi (task analysis), jonka tavoitteena on selvittää ja kuvata käyttäjän nykyiset tavoitteet, päämäärät, tehtävät ja työvaiheet kehitettävän palvelun tai järjestelmän osalta. (Takala-Schreib, 2012).

Myös protokolla-analyysi kuuluu kognitiivisiin menetelmiin. Pirita Seitamaa-Hakkarainen kuvaa protokolla-analyysia seuraavasti: 'Protokolla-analyysin eli ääneenajattelumenetelmän avulla tutkitaan yksilön ajattelu- ja ongelmanratkaisun taustalla olevia tiedonkäsittelyprosesseja.' (Seitamaa-Hakkarainen n.d.). Kun ajatellaan ääneen niin joku muu voi tarttua hyväksi havaitsemaansa ideaan ja kehittää sitä edelleen. Tätä menetelmää hyödynnettiin lähinnä työryhmän keskusteluissa.

Kolmas tähän menettelytapaan liittyvä menetelmä on tiedon hankinta eli yksinkertaisesti etsitään vastauksia julki tulleisiin kysymyksiin.

4.2 Tulosten keruu ja analysointi

Kysely julkaistiin kaikille Corenetin työntekijöille Corenetin Microsoft Sharepointin päälle rakennetussa intranetissä hyödyntäen Sharepointin omia kyselymahdollisuuksia. Vastauksia kerättiin kahden viikon ajan ja kyselystä tiedotettiin yleisesti intranetissä ja asiantuntijoita pyydettiin myös vastaamaan kyselyyn lähettämällä heille erillinen kutsu sähköpostitse.

Kyselyyn tuli vastauksia viideltätoista asiantuntijalta. Vastaukset kerättiin Microsoft Excel-taulukoksi, jota työstettiin helpommin ymmärrettävään muotoon erilliseen dokumenttiin. Kysely ja vastaukset on käsitelty tarkemmin erillisessä liitteessä 2, Opinnäytetyön kysely ja vastausten analysointi. Vastauksia analysoimalla saatiin rakennettua vaatimusmäärittely, ja sitä kautta muodostettiin myös varsinaiset valintakriteerit. Seuraavissa kappaleissa viitataan saatuihin vastauksiin ja niiden avulla tehtyihin määrittelyihin.

Perimmäiseen kysymykseen ”Tarvitaanko automaattista konfiguraationhallintajärjestelmää” saatiin 100 %:n kannatus eli asiantuntijan kokevat sen tarpeelliseksi.

Kyselyn työstämisen jälkeen oli ilmeistä, että ainakin seuraavat ehdottomat vaatimukset tulee asettaa valittavalle järjestelmälle:

1. Työkalun tulee pohjautua avoimeen lähdekoodiin, jota muokataan tarvittaessa. Tätä mieltä oli 66,7 % vastaajista.
2. Työkalun tulee tukea ainakin Cisco Systemsin sekä Alcatel-Lucentin laitteita. Laitteiston osalta reitittimien ja kytkinten tulisi olla tuettuina. Tästä vastaajat olivat melkein yksimielisiä.
3. Konfiguroinnit tulisi tapahtua ”Wizardilla” (53 % kannatus) tai vaihtoehtoisesti ”template”-mallia hyödyntäen (40 % kannatus).
4. Työkalun tulisi lisätä uusia laitteita järjestelmän piiriin automaattisesti autodiscover-menetelmällä. Työkalulle siis kerrotaan esimerkiksi tietty verkkoavaruus, josta se etsii laitteita. Ainoastaan neljä asiantuntijaa kannatti manuaalista lisäystä.
5. Varmuuskopiointisykli tulisi olla päivittäin tai heti, kun laitteen konfiguraatio on muuttunut. Asiantuntijat olivat tästäkin kysymyksestä lähes yksimielisiä.
6. Asiantuntijoille annettiin kyselyssä joukko ominaisuuksia, jotka heidän piti laittaa tärkeysjärjestykseen. Asiantuntijat nostivat muutosseurannan tärkeimmäksi toiminnallisuudeksi. Tämä on luonnollista, sillä kyseinen ominaisuus on erittäin tärkeä jokapäiväisessä työssä, konfiguraationhallinnan ja ongelmatilanteen selvittämisen kannalta.

Muita vähäisempiä vaatimuksia osaltaan olivat:

7. Ilmoitus vihamielisestä konfiguraatiomuutoksesta.
8. Laitteen konfiguraation poikkeavuuden tarkistus tulisi olla mahdollista.
9. Työkalun on tuettava laitteen ohjelmiston tarkistusta ja päivitystä, jotta voidaan varmistaa että ohjelmistoversio on samalla tasolla kuin muissa verkon laitteissa. Viimeksi mainitun vaatimuksen osalta on huomattava, että laitevalmistajat tarjoavat yleensä tähän omia, rinnakkaisia ratkaisuja. Laitevalmistajien omia ratkaisuja voitaisiin kenties hyödyntää, ellei konfiguraatiohallintajärjestelmä sisällä tämän kaltaista toiminnallisuutta.

Lisäksi tuotiin esille että hankkeen edetessä tulisi huomioida tukifunktiot, lisenssikulut ja muut implementointiin liittyvät kulut sekä itse implementaatioprojekti tulisi suunnitella ja toteuttaa asianmukaisesti.

5 VAATIMUSMÄÄRITTELYSTÄ VALINTAKRITEEREIHIN

Kyselyyn tulleiden vastausten analysoinnin pohjalta luotiin vaatimusmäärittely, joka löytyy liitteenä 1, Requirement specification, ja siitä edelleen valintakriteerit, jotka valmistajien tulee täyttää päästäkseen mukaan kilpailutukseen.

Valintakriteereiksi valittiin ehdottomia vaatimuksia, joiden on pakko täytyä, jotta työkalusta olisi jotain hyötyä. Mikäli yksikin pakollinen vaatimus jää täyttymättä, valmistaja putoaa pois kilpailusta eikä sitä huomioida valintatilanteessa. Kyselyn pohjalta luotiin myös optionaalisia määrittelyksiä, jotka osaltaan helpottavat työskentelyä ja osaltaan ovat hyvä lisä työkalulle – lisämäärittelysten täytyessä on odotettavissa että tuottavuus nousee ja tyytyväisyys järjestelmään kasvaa. Asiantuntijoilta saadut vastaukset ja kommentit toivat hyvän pohjan tarjouspyynnön (RFP – Request for Proposals) laatimiselle. Lisäksi jouduttiin myös miettimään, miten ja mitä loppujen lopuksi kysytään ja vaaditaan valmistajilta.

5.1 Tieto- ja tarjouspyyntö

Laajoissa valinta- tai kilpailutushankkeissa käytetään yleensä muun muassa tietopyyntöä (RFI- Request For Information) ja tarjouspyyntöä (RFP - Request For Proposals), joilla valmistajilta tai palveluntarjoajilta hankitaan tietoja ja tarjouksia päätöksenteon tueksi. Näiden tukena voidaan myös käyttää osallistumiskehotuksia, joiden avulla varmistetaan, että halutut tahot ovat tietoisia tarjousmenettelystä sekä voidaan varmistaa, että haluttu määrä valmistajia osallistuu tarjouskilpailuun.

5.1.1 Tietopyyntö - RFI

Tietopyyntö, RFI, on pääsääntöisesti tiedonkeruuprosessi, jossa valmistajalta, palveluntuottajalta tai muulta vastaavalta pyydetään tietoja tuotteen tai palvelun ominaisuuksista kirjallisessa muodossa. Tarkoituksena on usein saada lisätietoja varsinaisen tarjouspyynnön (RFP) laatimiseen. RFI toimii usein tarjouspyyntömenettelyn ensimmäisenä vaiheena. Yleinen käytäntö on että RFI:hin vastaavat tahot saavat varsinaisen tarjouspyynnön vastineeksi antamastaan informaatiosta. Tässä työssä RFI kuitenkin sivuutettiin, koska vaatimukset ovat varsin selkeät ja tiedetään, mihin tarpeeseen työkalu tulee. Kirjallisuudessa ja Internetissä törmää helposti myös RFC-termiin (Request for Comments), jota käytetään pääsääntöisesti standardointityössä eikä se täten liity tarjouskäsitteisiin.

5.1.2 Tarjouspyyntö - RFP

Tarjouspyynnön, RFP, tarkoitus on kertoa valmistajalle, että heidän tuotteelleen on kysyntää. RFP:n mukana lähetetään yleensä vaatimusmäärittelydokumentti, joka kertoo, mitä tuotteelta tai palvelulta vaaditaan. Valmistaja täyttää RFP:n ja vastaa siinä mahdollisesti oleviin kysymyksiin huomioiden mahdolliset poikkeavuudet ja erityisvaatimukset ja palauttaa RFP:n

täytettynä. RFP sisältää ne vaatimukset, jotka tuotteen on täytettävä, että se huomioidaan kilpailutuksessa. Lisäksi RFP määrittelee, missä muodossa vastaukset tulee toimittaa. Samalla asetetaan myös aikaraja, jonka sisällä vastaukset on toimitettava.

RFP käsittelee usein myös hintavaatimuksia, palvelusuorituksia, palvelutasovaatimuksia sekä mahdollisesti jopa sopimusteknisiä asioita. Monesti varsinkin hinnoittelu ja palveluvaatimukset lyödään lukkoon lopullisesti vasta sopimusneuvotteluissa.

RFI- ja RFP-käsittelyssä on suuria eroja julkisen ja yksityisen sektorin välillä. Julkisia kilpailutuksia koskee Suomen ja Euroopan Unionin hankintalait sekä kilpailulainsäädäntö. Yksityisellä sektorilla kilpailuttaminen on avointa ja säätelemätöntä ja siten yksinkertaisempaa kuin julkisella sektorilla. Suorahankinnat ja kilpailutuksen ohittaminen ovat myös täysin mahdollisia yksityisellä sektorilla.

Vaikka RFI onkin yleensä ensimmäinen vaihe tarjouspyyntömenettelyssä, tässä työssä aloitettiin suoraan RFP:llä. Täten tilanne käännettiin niin, että valmistajille lähetettiin suoraan vaatimukset ja samalla saadaan tietoja siitä, mihin valmistajien tuotteet pystyvät vaatimuksiin nähden.

6 VAIHTOEHDOT JA KILPAILUTTAMINEN

Tarjouspyynnön vastaanottajiksi valittiin viisi kappaletta avoimeen lähdekoodiin perustuvan työkalun tarjoajaa. Lisäksi mukaan valittiin kaksi kaupallista, valmiin työkalun tarjoajaa. Tarjouskilpailuun valittiin osallistujat karkean esikarsinnan myötä sekä vastuualueen liiketoimintajohtajan hyväksynnällä.

Näiden valmistajien ja heidän ohjelmistojensa kesken käydään kilpailutus, jonka avulla valitaan Corenetille parhaiten soveltuva vaihtoehto. Kilpailutuksen tavoitteena on huomioida vaatimukset, vastausten tasot, tukifunktiot sekä vaadittavat investoinnit esimerkiksi palvelimiin, lisensseihin sekä muihin vastaaviin. Itse käyttöönottoprojekti jää kuitenkin kilpailutuksen ulkopuolelle. Tarkoitus on että Corenet toteuttaa käyttöönoton itse omilla resursseillaan.

Mikäli tarjouksista käy ilmi että käyttöönotto olisi jotenkin hankalaa tai keskimääräistä haasteellisempaa, tulee asia kuitenkin huomioida valintatilanteessa, sillä tällöin käyttöönottoprojekti voi nostaa kokonaiskustannuksia sietämättömälle tasolle.

Valmistajille lähetettiin tarjouspyyntö saatekirjeellä varustettuna. Heille annettiin kaksi viikkoa vastausaikaa. Valmistajille annettiin myös mahdollisuus tehdä kysymyksiä tai tarkennuspyyntöjä tarjouspyyntöön liittyen. Määräaikaan mennessä tulleet hyväksytyt tarjouspyynnöt käsitellään ja vastaukset pisteytetään seuraavassa kappaleessa esitetyn mukaisesti.

Kolme valmistajaa oli yhteydessä lisäkysymysten osalta ja vastaukset toimitettiin kaikille valmistajille. Lisäksi kaksi valmistajaa oli yhteydessä tarjouskäsittelyn aikana tiedustellakseen etenemisestä ja mahdollisesta päättösaikataulusta.

7 PISTEYTYYS JA VERTAILU

7.1 Pisteytysmenetelmä

Vaatusmäärittelyssä mainittujen vaatimusten täyttymisestä jaetaan pisteitä. Pisteytyksen ja seulonnan jälkeen valitaan kolme korkeimmat pisteet saaneet vastaukset ja vertaillaan niitä keskenään. Pisteitä valmistajat saavat RFP:n täyttämistä ja palauttamisesta, vaatimusten täyttämistä ja optio-naalisista vaatimuksista saa lisäpisteitä.

Pisteytyksen pohjana käytettiin Yhdysvaltojen Idahon osavaltion hallinto-osaston (Idahon hallinto-osasto n.d.) määrittelemää ohjetta RFP:n arvioimiseksi, jota muokattiin hankintaan soveltuvaksi.

Pisteytys määräytyy alla olevan taulukon 2 mukaan. Koska valmistaja pu-toaa pois kilpailutuksesta, jos pakolliset määritteet eivät täyty, tässä osiossa pisteytys on: Hyväksytty / Hylätty.

Taulukko 2. Pisteytys

Pakolliset määritteet	Pisteytys
	Hyväksytty / Hylätty
Valinnaiset määritteet	Pisteytys
Täyttää vaatimukset	5
Täyttää vaatimukset osittain	3
Ei täytä vaatimuksia	0
Optiopisteet	Maksimipisteet
Hinnoittelu	10
Vastaus aikarajan sisällä	3
Yrityksen/yhteisön tausta	2
Organisaatorakenne	2
Kokemus (referenssit)	8
Vakavaraisuus	1
Yleinen laatu	1
Täydet optiopisteet	27
Pisteet yhteensä (min./maks.)	0/162

Kokonaisuudelle lasketaan pisteytyksen jälkeen painotettu pistearvo (weighted score) kaavalla 1:

$$y = \frac{n}{x} * z, \quad (1)$$

missä y on osallistujan painotetut/lopulliset pisteet eli, kuinka paljon pisteitä kyseinen osallistuja on saanut, n on osallistujan saamat pisteet, x on korkeimmat pisteet, mitä millekään osallistujalle on annettu ja z on maksimipisteet.

Mikäli maksimipisteet ovat esimerkiksi 500 ja kyseinen osallistuja on saanut 500 pistettä, on painotettu pistearvo 500 pistettä.

Lopullinen pistemäärä kaavan 1 mukaan on tällöin:

$$\frac{500}{500} * 500 = 500 \quad (1)$$

Mikäli maksimipisteet ovat esimerkiksi 500, toinen osallistuja on saanut 400 pistettä ja kyseessä oleva osallistuja on saanut 300 pistettä, on painotettu pistearvo samalla kaavalla laskettuna 375 pistettä.

$$\frac{300}{400} * 500 = 375 \quad (1)$$

Esitettyä pisteytysmenetelmää käytetään pisteyttämään tarjoajien vastaukset.

7.2 Osallistujien vertailu

Vastauksia saatiin valitettavasti vain kahdelta valmistajalta, vaikka alun perin kiinnostuksesta ilmoitti useampi taho. Koska tahoja on vain kaksi, verrataan näitä kahta tarjoajaa toisiinsa. Näistä valitaan toinen POC (Proof Of Concept) -vaiheeseen.

Taulukko 3. Tarjoajien vertailu ja pisteytys

	Tarjoaja 1	Tarjoaja 2
Perustiedot		
- Perustamisvuosi	1998	1996
- Liikevaihto	Noin 335 000 €	Ei ilmoitettu
- Henkilöstömäärä	Alle 200	2000
- Omistusmuoto	Valtion omistama + 20 yksityistä rahoittajaa	Yksityisessä omistuksessa
- Yrityksen asiakkaita	20 000	72 000
- Montako vuotta tuote ollut markkinoilla?	Beeta-vaihe on juuri päättynyt	4 vuotta
Peruspisteet		
	135	108
Optiopisteet (max.)		
Hinnoittelu (10)	1	10
Vastaus annetun aikarajan sisällä (3)	3	3
Yrityksen/yhteisön tausta (2)	1	2
Organisaatiorakenne (2)	1	2
Kokemus (8)	1	8
Vakavaraisuus (1)	1	1
Yleinen laatu (1)	1	1
Yhteensä (27)	9	27
Yhteispisteet		
	135 + 9 = 144	108 + 27 = 135
Painotettu pistearvo		
	155	136

Tarjoajan 1 pisteet määräytyivät siten, että kaikki perustason vaatimukset täyttyivät. Näistä vaatimuksista valmistaja sai 135 pistettä. Optiopisteitä tarjoaja 1 saa taulukon 2 mukaan seuraavaksi esitetyllä tavalla:

- Tarjoaja on pääosin suuntautunut valvontajärjestelmään, konfiguraationhallintajärjestelmä tullut rinnalle ja konfiguraationhallintajärjestelmä oli opinnäytetyön alkaessa beeta-vaiheessa. Tästä syystä tarjoajalle ei määritelty kuin 1 piste kokemuksesta ja referensseistä.
- Hinnoitteluosuudesta tarjoajalle annettiin 1 piste, koska ratkaisu on paljon kalliimpi kuin kilpailevat ratkaisut, hintatason ollessa moninkertainen kilpailijoihin nähden.
- Yhtiön vakavaraisuudesta annettiin 1 piste samoin kuin organisaatorakenteesta, lähinnä kehittäjien suuresta määrästä annettiin 1 piste. Tarjous annettiin aikarajaa seuraten, josta tuli 3 pistettä

Corenet vaatii konfiguraationhallintajärjestelmän tarjoajalta tarjouspyynnössä sekä peruskohtien, että mahdollisimman monen option täyttämistä. Tarjoaja 1 saa optio-osuudesta 9/27 ja peruspisteistä täydet 135 pistettä, jolloin kokonaispistemäärä on 144 pistettä.

Kokonaisuudelle lasketaan pisteytyksen jälkeen painotettu pistearvo (weighted score) aiemmin mainittua kaavaa käyttäen (kaava 1), joten tarjoaja 1 saa näin ollen pisteitä seuraavasti:

$$y = \left(\frac{144}{144}\right) * 162 = 162 \quad (1)$$

Tarjoajan 2 pisteet määräytyivät siten, että pakolliset vaatimukset täyttyivät muiden kohtien osalta, mutta ongelmakohtaksi nousi IPv6-tuki sekä kuormanjako eri järjestelmänoodien kesken. Tämä mahdollistaisi tarjouksen hylkäämisen. Tarjoaja 2 sai peruspisteiksi 108 pistettä. Optioista tarjoaja 2 sai taulukon 2 mukaan pisteitä seuraavana esitetyn tavan mukaan:

- Tarjoajan 2 tuote on ollut markkinoilla jo 4 vuotta ja siihen tulee päivityksiä tasaisella tahdilla. Lisäksi tarjoajalla 2 oli esittää referenssejä, joten kokemuksesta tuli 8 pistettä.
- Hinnoittelusta tarjoaja 2 saa täydet 10 pistettä, koska se on erittäin edullinen kilpailijoihinsa nähden.
- Taustasta ja organisaatorakenteesta tarjoaja saa molemmista täydet 2 pistettä. Vastaus annettiin myös annetun aikarajan sisällä, joten siitä tulee 3 pistettä. Vakavaraisuudesta tulee 1 lisäpiste.

Tarjoaja 2 saa optio-osuudesta täydet 27 pistettä ja peruspisteistä 108 pistettä. Yhteispisteet ovat näin ollen 135.

Painotettu pistearvo on siis kaavan 1 mukaan:

$$y = \left(\frac{135}{144}\right) * 162 = 152 \quad (1)$$

7.3 Lopullinen yhteenveto

Ensimmäinen tarjoaja voittaa tarjousvertailun pisteiden osalta. Tarjoaja kaksi voitaisiin tiputtaa tarjousvertailusta, sillä se ei täytä kaikkia perusvaatimuksia. Kuitenkin jo tarjouspyyntöä laadittaessa kyseessä olevat ominaisuudet (IPv6-tuki sekä kuormanjako-ominaisuudet) eivät olleet ensisijaisia, mutta katsottiin hyväksi, että tarjoaja täyttäisi nekin.

Mikäli yrityksissä jouduttaisiin seuraamaan samoja kilpailutusta koskevia lakeja kuin julkinen sektori, olisi ratkaisu yksinkertainen. Tarjoaja 2 tiputettaisiin pois tarjouksen yhteensopimattomuuden takia ja tarjoaja 1 voittaisi tarjouskilpailun. Koska yhteensopivia tarjouksia on saapunut vain yksi, olisi julkisella sektorilla tällöin kaksi vaihtoehtoa:

- a) Tarjouspyyntö hyväksytään sellaisenaan, toteutetaan POC ja aloitetaan sopimusneuvottelut
- b) Julistetaan uusi tarjouskilpailu, koska haluttu hintataso ylittyi

Koska kyseessä kuitenkin on suljettu tarjouskilpailu yritysten kesken, valinta jää projektin ohjausryhmän päätettäväksi. Päätöksiä varten tulee valmistajien antamia tarjouksia tarkentaa asettamalla lisäkysymyksiä, joille annetaan vastausaika. Tämän jälkeen tilanne tarkistetaan uudelleen ja ohjausryhmälle annetaan tiedot päätöksentekoa varten. Tarjoaja 2:lta on tiedusteltava uupuvien vaatimusten mahdollisesta täyttämisestä, sekä miten ne voisivat sitoutua niiden toteuttamiseen Corenetin sopimuskumppanina. Tarjoajalta 1 on tiedusteltava työkalun rakennetta ja sitä, sisältääkö hinta ylimääräisiä komponentteja vai kaiken tarvittavan. Annettujen tietojen perusteella järjestelmä rakentuu useista eri komponenteista, joita yhdistämällä saadaan katettua Corenetin asettamat vaatimukset kun sitä vastoin tarjoaja 2:n ohjelmisto täyttää vaatimukset perusjärjestelmällä (lukuun ottamatta mainittuja puutteita).

Saadut vastaukset verrataan tässä keskenään pisteytyksen perusteella:

Taulukko 4. Lopulliset pisteet ja niiden vertailu

Yhteispisteet		
	$135 + 9 = 144$	$108 + 27 = 135$
Painotettu pistearvo		
	162	152

Pistemäärät eivät kuitenkaan aina kerro sitä kumpi olisi parempi työkalu yritykselle. Täytyy ottaa myös huomioon tarjoajien tulevaisuuden suunnitelmat eli mitä päivityksiä ja lisäyksiä työkaluun on mahdollisesti tulossa. Nämä lisäykset mahdollisesti kattavat sellaiset asiat, joista nyt ei saanut pisteitä. Lisäksi ei ole aina helppo päätellä onko vastaaja ymmärtänyt kysymyksen tai vaatimukset niin kuin kilpailuttaja on tarkoittanut. Tästä syystä kannattaa järjestää kuulemistilaisuus, jossa tarjoajat voivat esittää ratkaisunsa sekä perustelunsa esitettyihin valintoihin ja tarjoukseen.

Toisaalta kyseessä on eri yritysten tuottamia erilaisia työkaluja, jotka toimivat hyvinkin samalla tavalla, mutta eroavaisuuksiakin löytyy. Nämä eroavaisuudet erottavat kilpailijat toisistaan. Harvemmin yksi ja sama työkalu sopii kaikille – kaikki tarvitsevat jotain erilaista.

Jotta voidaan varmistaa työkalun sopiminen Corenetin käyttöön, on pisteyttämisen lisäksi käytettävä tarjouspyyntöön sisällytettyä mahdollisuutta suorittaa testausta Corenetin liiketoimintaympäristössä. Soveltuvuustestaus tehdään POC-menettelyllä.

8 POC (PROOF OF CONCEPT)

POC, eli 'Proof Of Concept -menetelmä voi olla vaihtoehto toimivalle prototyypille tai yksi tuotekehityksen vaihe ennen toimivan prototyypin laatimista. Proof Of Concept voitaisiin kääntää vaikkapa 'idean toiminnalliseksi validoinniksi', sillä se on tavallisesti teoreettinen tai käsitteellinen esitys, joka todistaa, että tuoteidea on toteutettavissa.' (Yritys-Suomi n.d.).

Palvelu- ja ohjelmistotuotannossa POC-termiä käytetään usein tarkoittaessa järjestelmän soveltuvuustestausta yrityksen jokapäiväisessä toiminnassa ennen varsinaista hankintaa tai sopimuksen allekirjoittamista.

Corenet sisällytti tarjouspyyntöön vaatimuksen saada suorittaa maksuton soveltuvuustestaus ennen lopullista valintaa. Soveltuvuustestaukseen valitaan kilpailutuksen perusteella se valmistaja, jonka tuote vaikuttaisi soveltuvan parhaiten Corenetin käyttöön. Kyseisen valmistajan tarjoama työkalu asennetaan virtuaaliympäristöön, jonne ohjataan valittu osa Corenetin omasta tai testiasiakkaan verkosta. Ideana on saada käsitystä siitä, kuinka hyvin valmistajan työkalu toimii ja miten hyvin se vastaa asetettuja määritelmiä oikeassa elämässä – testataan siis järjestelmän rajat. Testauksen myötä saadaan selville työnkulku kyseisen työkalun avulla ja kartoitetaan kaikki käyttötavat.

Testauksen tarkoituksena on lisäksi selvittää myös subjektiivisia asioista, kuten sovelluksen tai järjestelmän nopeus, käytettävyys ja käyttöliittymän toimivuus. On myös tärkeää selvittää, miten järjestelmä toimii, kun useat käyttäjät käyttävät sitä samaan ja eri aikaan. Lisäksi on selvitettävä, millaisia erilaisia käyttäjärooleja ja valtuuksia työkalu tukee. Ennen kaikkea halutaan tietenkin selvittää, auttaako kyseessä oleva sovellus loppukäyttäjää suoriutumaan tehtävistään paremmin ja nopeammin kuin aiemmin. Pääasia kuitenkin on, että loppukäyttäjät ovat valmiita käyttämään työkalua.

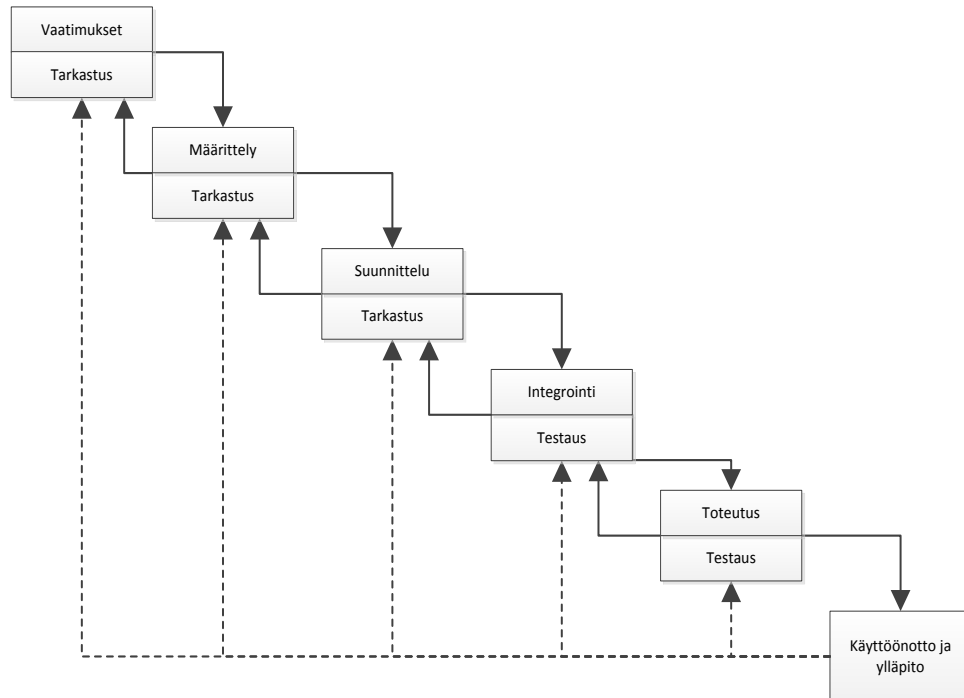
POC-vaiheessa on myös tärkeää testata, miten yhteistyö toimii työkalun toimittajan ja loppukäyttäjän (Corenetin) kesken. Osapuolten tarpeet ja niiden priorisointi on selvitettävä. Tarkemmin sanottuna tulee selvittää Corenetin mahdollisesti vaatimien muutoksien vaikutusmahdollisuudet tuotekehitykseen. POC-vaiheessa halutaan tietää, että valmistaja on valmis tukemaan loppukäyttäjää ja loppukäyttäjän tarpeita.

Jotta voidaan kerätä tarpeeksi tietoa ja että voidaan huomioida käyttötarpeet riittävällä tasolla, POC-vaihe kestää noin kuukauden. Tämän jälkeen soveltuvuustestauksen onnistumista tulee arvioida. Arvioinnissa kiinnitetään erityistä huomiota testikäyttäjien antamaan palautteeseen ja mahdollisiin puutteisiin. Puutteet käydään läpi tarjoajan kanssa.

Mikäli puutteet ovat korjattavissa tai niiden merkitys on pieni, voidaan onnistuneen POC:n jälkeen siirtyä sopimus- ja tilausneuvotteluihin. Onnistuneen tai hyväksytyn POC:n kriteerit tulee asettaa POC:n alkuvaiheessa, jotta varmistetaan, että etenemistä voidaan seurata riittävällä tasolla ja kaikille osapuolille on selvää, mitä POC:ilta haetaan. POC tai sen hyväksymiskriteeristön asettaminen ei ole osa tätä lopputyötä.

9 ELINKAARIHALLINTA

”Tuotteella on elinkaari, joka alkaa tuotteen kehitystyöstä ja päättyy tuotteen myynnin vähenemiseen ja tuottojen putoamiseen” (Taloussanomat n.d.).



Kuva 2. Yksi elinkaarihallinnan malleista; vesiputousmalli

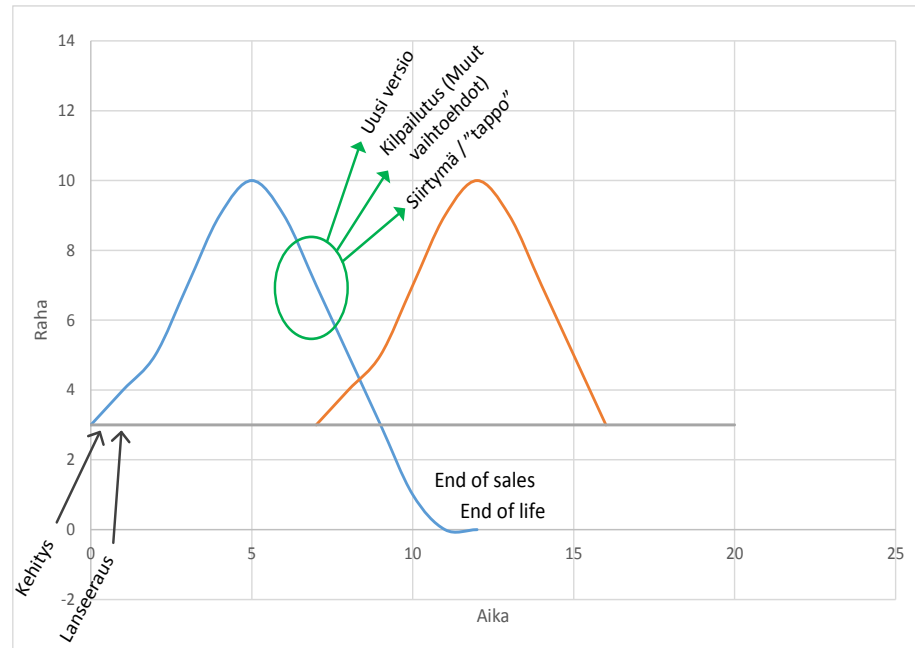
Elinkaarihallinnassa täytyy ottaa huomioon päivitykset, päivityssykli ja –tapa, sekä odotettavissa oleva elinikä ohjelmistolle ja investoinnille. ROI (Return of Investment) tulee myös ottaa huomioon eli, miten nopeasti tehty panostus maksaa itsensä takaisin. Elinkaarimallissa on myös huomioitava, miten saadaan halutut tiedot siirrettyä mahdolliseen uuteen ohjelmistoon vanhasta luovuttaessa, missä näitä tietoja säilytetään sekä kuka tiedon omistaa.

Myös työkalulle saatavilla oleva tuki tulee huomioida ja arvioida. Työkalun tarjoajan ollessa toisesta maasta tai jopa toiselta mantereelta on otettava huomioon muun muassa aikaero.

Jossain vaiheessa tuote myös saattaa tulla tiensä päähän, jolloin tarvitaan tilalle uusi, vastaava tuote. Tuote itsessään ei kuole koskaan, mutta se voi tulla tarpeettomasti seuraavien skenaarioiden toteuduttua:

- Käyttöympäristö muuttuu niin, ettei työkalua voida enää käyttää
- Löydetään uusi ja parempi menetelmä tehdä työkalun tekemät asiat
- Tarve työkalulle loppuu
- Työkalu integroidaan toiseen
- Työkalun kehittäminen loppuu

(Wikipedia n.d.)



Kuva 3. Tuotteen elinkaari

Kuvassa 3 sininen viiva kuvastaa ensimmäistä tuote- tai palvelusukupolvea ja oranssi viiva kuvastaa seuraavaa tuotesukupolvea tai tuotetta. Kehitykseen ja lanseeraukseen kuluu tietty määrä resursseja, kuten aikaa ja rahaa. Tällöin on tärkeää pysyä kokoajan vakaasuorassa kulkevan kannattavuusrajan yläpuolella, että välttyttäisiin tappioilta. Aluksi vain tietyt yritykset tai käyttäjät ottavat tuotteen tai palvelun käyttöönsä (niin sanotut ”early adopters”), mutta tuotteen lanseerauksen jälkeen on odotettavissa nousua myynnissä, mikäli tuote on saanut hyvää palautetta ja tuotteen markkinointi onnistuu. Samalla luonnollisesti kannattavuus tai tuotto paranee.

Nousua tapahtuu tietyn ajan ja ennen pitkää saavutetaan huippu, saturaatiopiste, jolloin tuote joutuu kovempaan kilpailuun eikä uusia asiakkuuksia oikein synny. Saturaatiotilan jälkeen alkaa vääjäämättä lasku. Valmistajat yrittävät luonnollisesti paikata laskevaa kannattavuutta tai menekkiä lanseeraamalla uuden tuotteen tai palvelun (oranssi viiva kuvassa 3). Valmistajan päättäessä ajaa tuote alas, sille julistetaan ensin end-of-sales (EOS). Tämän jälkeen tuotetta ei enää myydä ja varsinaisen tuotetuen loppuessa julistetaan sille end-of-life (EOL), eli elinkaaren loppu, jolloin asiakkaiden on siirryttävä muun tuotteen käyttämiseen. Parhaimmassa tapauksessa EOS:n ja EOL:n välillä on useita vuosia aikaa reagoida tilanteeseen. Esimerkiksi lähiverkkokytkimien osalta myynnin loppuessa laitetta tuetaan vielä 2-3 vuotta ennen kuin sen elinkaari loppuu.

Kun Corenetin valitseman työkalun elinkaari siirtyy laskuosuudelle, on Corenetin päätettävä, siirrytäänkö uuteen versioon, järjestetäänkö uusi kilpailutus vai ajetaan työkalu kokonaan alas. Mikäli Corenet päivittää työkalun uuteen versioon, päästään taas uudelle nousuosuudelle (oranssi viiva kuvassa 3).

Mikäli Corenet päätyy järjestämään uuden kilpailutuksen, tilanne joudutaan luonnollisesti aloittamaan alusta uusien vaihtoehtojen käyttöönotossa ja tuotteen sijainti elinkaarikäyrällä joudutaan tutkimaan tarkasti. Sama koskee siirtymistä täysin uuden työkalun käyttöön, jolloin vanhasta luovutaan. Molemmissa tapauksissa joudutaan huomioimaan uuden työkalun käyttöönotossa vanhojen tietojen siirto uuteen järjestelmään sekä käyttöönotto-projektin mahdollisesti vaatimat muutokset prosesseihin, käyttöön tai muuhun vastaavaan. Optimitilanne olisi, jos työkalu tukisi nykyisiä prosesseja. Tällöin on kaikkein pienin vastustus tuotteen käyttöönotolle.

Huolellisella suunnittelulla voidaan tuotteen elinkaari huomioida jo valintavaiheessa ja varmistaa että on olemassa jonkinlainen suunnitelma, kuinka menetellään, mikäli työkalusta luovutaan ja kuinka siirrytään uuden työkalun käyttöön. Nykyisin investoinnille ei kuitenkaan tarvitse tuottaa elinkaarisuunnitelmia kuin 3-10 vuodelle, kymmenen vuoden ollessa jo erittäin pitkä aika. Useimmiten käytetään 3 tai 5 vuoden suunnitelmia, joita on helppo sisällyttää esimerkiksi osaksi käyttöönottosuunnitelmia.

Corenetille tarjotut työkalut olivat siinä mielessä hyviä, että molempien valmistajien ohjelmistot ovat elinkaaren alussa, nousuosalla. Toinen on juuri lanseerattu ja toinen ei ole vielä saavuttanut saturaatiopistettä. Näin ollen kumpi tahansa työkalu voidaan olettaa olevan käytettävissä seuraavat 3-5 vuotta ilman suurempia huolia työkalun/ohjelmiston vanhenemisesta tai poistumisesta markkinoilta.

10 LOPPUSANAT

Konfiguraationhallinta oli erittäin mielenkiintoinen aihe opinnäytetyöksi, koska sen automatisoinnilla voidaan varmistaa myös verkohallinnan tulevaisuus ja huomattavasti paremmat työskentelyedellytykset asiantuntijoille.

Työn aikana pääsin osallistumaan sovelluskehityshankkeeseen, joka sisälsi sekä vaatimusmäärittelyn, kilpailutuksen että vertailun. Erityisen kiinnostavana koin hankkeen siksi, että saan seurata, miten tämä ratkaisu implementoituu osaksi yrityksen arkea. Mielenkiintoista tämä on lisäksi siksi, että yrityksellä on jo runsaasti kokemusta verkkolaitteiden konfiguroinnista, hallinnasta ja valvonnasta.

Opinnäytetyötä edeltänyt reilun vuoden kestäneen työskentelyn valvontasovellusten ja tämän hetkisten konfiguraationhallintatyökalujen parissa antoi riittävät perustiedot ja kokemuksen alasta ja verkkolaitteiden hallinnasta. Työssä pystyin siis hyödyntämään omakohtaisia kokemuksia sekä koulusta että työpaikan kautta saatua pohjatietoa.

Työ antoi hieman erilaisen näkemyksen tietoliikenneinsinöörin mahdollisista työnkuvista. Työ murtaa erinomaisesti sen stereotypian, mikä IT-insinööreistä on. Kaikki työ ei olekaan pelkkää ohjelmointia tai verkkolaitteiden ylläpitoa, vaan siihen voi sisältyä huomattavan paljon muutakin, kuten tavoiteasetantaa ja seurantaa.

Työn aikana perehdyin konfiguraationhallinnan, elinkaarihallinnan ja erilaisten konfiguraationhallinnan työkalujen lisäksi vahvasti myös tarjouspyyntöjen tekemiseen, vastausten pisteyttämiseen, tulevan työkalun valintaan, sen käyttöönottoon ja mukauttamiseen. Koska olen itse perehtynyt enemmän tietoliikennemaailmaan ja ohjelmointiin, niin työ osoittautui myös välillä melko haasteelliseksi.

Työ itsessään oli hyvin arvokas eritoten oppimisprosessina. Opin paljon uusia asioita. Konfiguraationhallinta osoittautui hyvin laajaksi alueeksi puhumattakaan siitä, mitä kaikkea täytyy ottaa huomioon jos yritykselle valitaan jokin tuote, joka tulee päivittäiseen käyttöön.

Työssä saavutettiin mieluisa lopputulos ja Corenetille löydettiin hyviä ehdokkaita, jotka tarjoavat uusia konfiguraationhallintatyökaluja. Lopullinen valinta seuraa POC:ia ja se käydään Corenetin sisäisesti eikä lopputyö siten käsittele tätä osuutta. Toki toivon pääseväni osallistumaan myös POCiin ja vaikuttamaan lopulliseen valintaan.

Corenet tarjosi erittäin hyvät puitteet työn suorittamiseen. Erityiskiitoksen haluan antaa työpaikkaohjaajalleni Jan Enlundille, kannustuksesta työn aikana ja ohjauksesta oikeaan suuntaan, kun tuntui että päädyin umpikujaan.

Kiitokset myös ystäväilleni ja avopuolisolleni tuesta, rohkaisusta ja kannustuksesta.

LÄHTEET

Alcatel-Lucent, Satumäki, Koulutus, 2013

Cisco Systems, Network Configuration Management, Viitattu 03.06.2013
http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.pdf

Idahon valtio, Guidelines for Developing and Evaluating a request for proposal, Viitattu 12.07.2013
http://purchasing.idaho.gov/pdf/publications/guidelines_for_rfp.pdf

Itä-Suomen Yliopisto, Vaatimusmäärittely, Viitattu 03.06.2013
<http://cs.joensuu.fi/tSoft/vaatimusmaarittely.htm>

ManageEngine, DeviceExpert, Viitattu 03.06.2013
<http://www.manageengine.com/products/device-expert/>

Mike Rothman, Securosis – Vulnerability Management Evolution, Viitattu 04.06.2013.
https://securosis.com/assets/library/reports/Securosis-Vulnerability-Management-Evolution_FINAL-multi.pdf

Opmantek, opConfig, Viitattu 03.06.2013
<https://opmantek.com/network-configuration-management-opconfig/>

Puppet Labs, Puppet Device, Viitattu 03.06.2013
<http://puppetlabs.com/solutions/configuration-management>

Seitemaa-Hakkarainen, Protokolla-analyysi, Viitattu 12.07.2013
http://www.metodix.com/fi/sisallys/04_virtuaalikirjasto/dokumentit/aineistot/protokollaanalyysi

Shrubbery Networks Inc, RANCID, Viitattu 03.06.2013
<http://www.shrubbery.net/rancid/>

Susan Dart, The Past, Present, and Future of Configuration Management, cm_past_pres_future_TR08_92.pdf, 1992, Viitattu 03.06.2013
<http://repository.cmu.edu/sei/229/>

Taloussanomien www-sivut, Elinkaari. Viitattu 03.11.2013.
<http://www.taloussanomien.fi/porssi/sanakirja/?termi=elinkaari>

Vuokko Takala-Schreib, Tehtäväanalyysi. Viitattu 12.07.2013
<http://fnoll.wordpress.com/2012/08/20/tehtavaanalyysi/>

Ward Holloway, Configuration Management = Risk Management, Viitattu 04.06.2013
<http://www.firemon.com/blog/configuration-management-risk-management>

Wikipedia, Flame, Viitattu 03.06.2013
[http://en.wikipedia.org/wiki/Flame_\(malware\)](http://en.wikipedia.org/wiki/Flame_(malware))

Wikipedia, Konfiguraationhallinta, Viitattu 26.05.2013
http://fi.wikipedia.org/wiki/Ohjelmiston_versiohallinta#Konfiguraationhallinta

Wikipedia, Ohjelmiston elinkaaren vaiheet, Viitattu 12.07.2013
http://fi.wikipedia.org/wiki/Ohjelmistotuotanto#Ohjelmiston_elinkaaren_vaiheet

Wikipedia, Riskienhallinta, Viitattu 04.06.2013
<http://fi.wikipedia.org/wiki/Riskienhallinta>

Wikipedia, Stuxnet, Viitattu 03.06.2013
<http://en.wikipedia.org/wiki/Stuxnet>

Yritys-Suomen www-sivut, Proof of Concept, Viitattu 12.07.2013
http://www.yrityssuomi.fi/web/guest/aihe?pp=polku_TuotejaPalvelukehitys&ppa=palp_Idean_tuotteistaminen&aihe=1000170

HAASTATTELUT

Danielsbacka, J. 2013. Tietoliikenneasiantuntija. Corenet Oy. Henkilökohtainen tiedonanto 2013.

Enlund, J. 2013. Asiakkuuskehittäjä. Corenet Oy. Henkilökohtainen tiedonanto 2013.

Löytynoja, A. Järjestelmäasiantuntija. Corenet Oy. Henkilökohtainen tiedonanto 2013.

Tiensuu, M. 2013. Johtaja. Corenet Oy. Riihimäki. Haastattelu 2013.

Tiilikainen, V. Tietoliikenneasiantuntija. Corenet Oy. Henkilökohtainen tiedonanto 2013.

LIITTEET

Requirement specification

Liite 1

Opinnäytetyön kysely ja vastausten analysointi

Liite 2



Requirement specification

TBa, JEn

Table of contents

1 PURPOSE OF THIS DOCUMENT	3
2 DEFINITIONS	3
3 BIDDER INFORMATION	3
4 SYSTEM MANUFACTURER SUPPORT REQUIREMENTS.....	3
4.1 Requirements	3
4.1.1 Mandatory requirements for OEM support	4
4.1.2 Optional requirements for OEM support	4
4.1.3 Optional hardware support requirements	4
4.1.4 Further OEM support	5
5 SUPPORTED STANDARDS	5
6 SECURITY	5
6.1 Mandatory requirements	5
6.2 Optional requirements	5
7 ENVIRONMENT	5
7.1 Mandatory requirements	5
7.2 Optional requirements	6
7.3 Fault tolerance	6
7.4 Fault recovery	6
8 RELIABILITY REQUIREMENTS	6
9 USABILITY REQUIREMENTS	6
9.1 Requirements	6
9.1.1 Mandatory requirements	6
9.1.2 Optional requirements	7
10 MAINTENANCE REQUIREMENTS	8
11 IN-HOUSE CHANGES AND LICENSING	8
12 TESTING	8
13 REFERENCES	8
14 PRICING	8
15 ANSWERING QUESTIONS AND REQUIREMENTS	9

1 PURPOSE OF THIS DOCUMENT

This document includes the requirement specifications for Corenet's request for proposals (RFP) regarding Network Configuration Management tools and/or systems.

The purpose of this document is to define Corenet's needs and requirements so the manufacturer can answer directly to the RFP. This document is also used as an attachment to a Bachelor's Thesis.

The RFP contains mandatory requirements and optional requirements and are marked accordingly.

2 DEFINITIONS

Mandatory requirement – System has to fulfill the set requirements to be noted in the selection process.

Optional requirement – It is highly recommended that the system meets the optional requirements. Failing in meeting the optional requirements will not directly affect the final decision.

Scoring – Given answers will be scored so that points are granted if requirements are met and there is also a possibility to get additional points by meeting the optional requirements. Total score is 100 points. Scoring procedure will not be disclosed to candidates.

3 BIDDER INFORMATION

Please give a short presentation of the company or organization. State information such as number of employees, when the company was established, and how long the company has been developing the configuration management system. Also state how much of the revenue is invested in product development. Please enclose a copy of latest financial statement and key figures from latest fiscal year.

4 SYSTEM MANUFACTURER SUPPORT REQUIREMENTS

4.1 Requirements

The main goal is to choose a network configuration tool for Corenet that can manage configurations automatically, take backups (to a server, for example), do configuration restorations, manage software versions together with an interface for these actions and has the capability to do mass configurations. The basic system requirements are related to direct manufacturer support. Corenet requires mandatory support for several manufacturers, since Corenet's networks include multi-vendor devices. The OEM support should include the majority of the manufacturer's devices (>80%).

The optional hardware support requirements focus mostly on wireless devices and secondly on fire-wall support.

4.1.1 Mandatory requirements for OEM support

4.1.1.1 Support for Cisco Systems' equipment

Switches
Routers

4.1.1.2 Support for Alcatel-Lucent's equipment

Switches
Routers

4.1.2 Optional requirements for OEM support**4.1.2.1 Support for Hewlett-Packard's equipment**

Switches
Routers

4.1.2.2 Support for Extreme Networks' equipment

Switches
Routers

4.1.2.3 Support for Juniper Networks' equipment

Switches
Routers

4.1.3 Optional hardware support requirements**4.1.3.1 WLAN access points**

Cisco Systems
Alcatel-Lucent
Hewlett-Packard
Enterasys

4.1.3.2 WLAN controllers

Cisco Systems
Alcatel-Lucent
Hewlett-Packard
Enterasys

4.1.3.3 Firewalls

Cisco Systems
Juniper Networks
F5
Checkpoint

4.1.3.4 Load balancers

Cisco Systems
Juniper Networks

4.1.3.5 Content filtering

Cisco Systems/Ironport
Bluecoat

4.1.4 Further OEM support

Please indicate how OEM support can be developed for manufacturers not mentioned in previous sections, for instance Huawei, Brocade etc. Also indicate issues related to in-house development if Corenet should choose to develop support on its own, for instance what kind of support Corenet should require from the manufacturers, devices, in which language the code should be written and what kind of support you are able to offer during such development (support forums, knowledge base etc.).

5 SUPPORTED STANDARDS

Please indicate which standards the configuration management system supports or follows, for instance SNMPv1/SNMPv2.

6 SECURITY

6.1 Mandatory requirements

- strong administrator rights
- change history
- personal username and password
- support for user hierarchy (admin, groups, users)

6.2 Optional requirements

- own limited view for the customer
- support for Radius, LDAP, TACACS++
- support for strong authentication

7 ENVIRONMENT

7.1 Mandatory requirements

Support for Windows or Linux server environment (32 or 64bit). Support for installation in virtual environments. Please indicate installation requirements (memory, disk space and processor capacity) as well as additional installation needs, for instance, database requirements. Please state how system backups can be done, for instance backing up configuration database and system to a SAN (Storage Area Network).

7.2 Optional requirements

Ready-to-install VMware image.

7.3 Fault tolerance

The system must support server clustering or load balancing. Please indicate the most efficient fault tolerant setup (cluster, hot standby, load balancing etc.).

7.4 Fault recovery

The system has to be up and running as soon as possible after fault/boot.

Indicate failover time in fault tolerant environment described in previous section.

8 RELIABILITY REQUIREMENTS

Please state the following:

For how long has the software been available?

How many different versions have been published?

What is the update cycle? (Yearly main releases etc.)

How many users does the software have worldwide and in Finland?

9 USABILITY REQUIREMENTS

9.1 Requirements

The configuration management systems should be possible to easily integrate into Corenet's main support processes. Corenet's processes are built on ITIL v6 definitions (Information Technology Infrastructure Library). Please state if ITIL processes have been considered when developing the system or if such integrations have been made by any customers.

Since Corenet as an integrator is handling its customer's networks, the systems should support multi-tenancy, i.e. Corenet should be able to serve several customers using the same centralized configuration management system. Please indicate if the configuration management system supports multi-tenancy. If not supported, indicate how such a support could be achieved.

Please state open system APIs and integration possibilities to other systems, like for instance extranets and intranets.

9.1.1 Mandatory requirements

9.1.1.1 Grouping of devices

The system should be able to group devices:

- by customer
- by manufacturer
- by IP network
- by device type (switch, router etc)
- combination of above mentioned groups

9.1.1.2 Device search

The system should include search capabilities, so that a specific device can be found in the network. Search criteria should include:

- device name
- device MAC address
- device IP
- device type
- customer name

9.1.1.3 IPv6 support

Please state if the configuration management system supports IPv6.

9.1.1.4 Backup of device configuration

The configuration management system must support backing up device configurations. Please indicate supported backup types (internal/external database) and database type. Also indicate how a database can be moved or transferred to additional systems (database dump, csv-file (comma separated value) etc.). The systems should clearly indicate when a device has last been backed-up. If back-up has failed the system should indicate time of failure and reason. The system should also indicate when the next scheduled back-up run is taking place.

The configuration management system must support backup scheduling. Please indicate possible ways of automating backup (monthly, weekly daily, backup on configuration change etc.)

9.1.1.5 Mass configuration

The software must support mass configuration, i.e. small configuration changes to a multitude of devices in a customer's network. Please indicate how mass configuration is supported? Can mass configuration functions be scheduled?

9.1.1.6 User support

Please indicate how end users and administrators are supported. Describe how bug reports are done and how they are treated as well as technical support requests. Please state if support is available in Finland or in Finnish.

9.1.1.7 Training and certification

Please describe what kind of training is available to end users. If a certification process exists, please describe the process and different levels of certification and certification costs. Please indicate if training material is readily available and if self-training is possible.

9.1.2 Optional requirements

The configuration management system should include capabilities for making device policies, for instance policies including SNMP group values, IP address values and the alike. The system should raise an alarm if device policies are not met (hostile changes or hostile configuration). Please state if systems support these optional requirements.

10 MAINTENANCE REQUIREMENTS

The configuration management system must support configurations backups, as stated in section 7.1. Furthermore the system must support audit trailing, i.e. change tracking – when changes were made, who made the changes (authorized change/unauthorized). The audit information should be possible to store in a database, and the database must be searchable. Additionally the system should support the use of external databases. Please indicate how support for audit trailing is carried out in the system and what types of databases are supported.

11 IN-HOUSE CHANGES AND LICENSING

Please indicate what type of licensing is used with the system. Does Corenet have the right to complete changes on its own and must all changes be made publicly available? Are there preferred partners to make changes to the existing system code?

12 TESTING

Corenet must be able to test the configuration management system in a laboratory environment before deployment. The tool must be reliable as Corenet operates crucial networks. Please indicate possibilities to make a PoC (proof of concept) testing and what kind of support you can give Corenet during the testing phase.

13 REFERENCES

Please state system references, especially operators and integrators.

14 PRICING

Corenet is searching for a configuration management system with low costs during the whole lifecycle (deployment, running and upgrading) as well as a simple pricing mechanism. Please indicate systems pricing or if the system software is free, indicate pricing according to deployment needs (setup) in the following scale:

- 500 devices
- 1000 devices
- 2000 devices
- 5000 devices
- 10 000 devices
- over 10 000 devices
- over 50 000 devices

15 ANSWERING QUESTIONS AND REQUIREMENTS

Corenet has attached a Microsoft Excel-worksheet to the RFP. Please state your answers in the Excel-file. For the mandatory requirements, state answers only as "yes" or "no". If support is being developed, then please state additional information in the additional field and answer "partly".

If using additional attachments, please number attachments starting from number one and refer to the attachment from within the Excel-file or from your tender.

Corenet expects to receive the following files:

- Tender including short presentation of company/organization
- Financial statement and key figures from latest fiscal
- Completed MS Excel-file
- any additional attachments used or referred to in the tender



Opinnäytetyön kysely ja vastausten analysointi

TBa, JEn

SISÄLLYS

1	KYSELY JA SIITÄ SAADUT VASTAUKSET	3
1.1	Tarvitaanko automaattista konfiguraationhallintajärjestelmää?.....	4
1.2	Millainen konfiguraatiohallintajärjestelmän tulisi olla?	5
1.3	Mitä eri laitteita konfiguraatiohallintajärjestelmän tulee tukea?.....	6
1.4	Minkä valmistajan laitteita järjestelmän tulee tukea?	7
1.5	Miten toivoisit esi-/loppukonfiguraation tapahtuvan uusissa asennuksissa?	8
1.6	Miten uudet laitteet tulisi lisätä järjestelmään?	9
1.7	Millä syklillä laitteista otetaan varmuuskopio?.....	10
1.8	Miten tärkeäksi koet seuraavat asiat?	11
1.9	Mihin varmuuskopiot olisi mielestäsi hyvä siirtää laitteelta?	12
1.10	Mitä muuta tulisi järjestelmää hankittaessa sinusta huomioida?	12
1.11	Sana on vapaa - voit antaa muita mieleen juolahtaneita kommentteja.	12
2	PIKAINEN YHTEENVETO TULOKSISTA	13
2.1	Ehdottomat vaatimukset vastausten perusteella	13

Kysely ja siitä saadut vastaukset

Kysely suoritettiin aikavälillä 01.4. – 10.4.2013 Corenetin intranetissä, joka rakentuu Microsoft Sharepoint-palvelun päälle. Itse kysely toteutettiin Sharepointista valmiina löytyvällä työkalulla, koska siinä oli riittävät valmiudet kyselyn toteuttamiseksi.

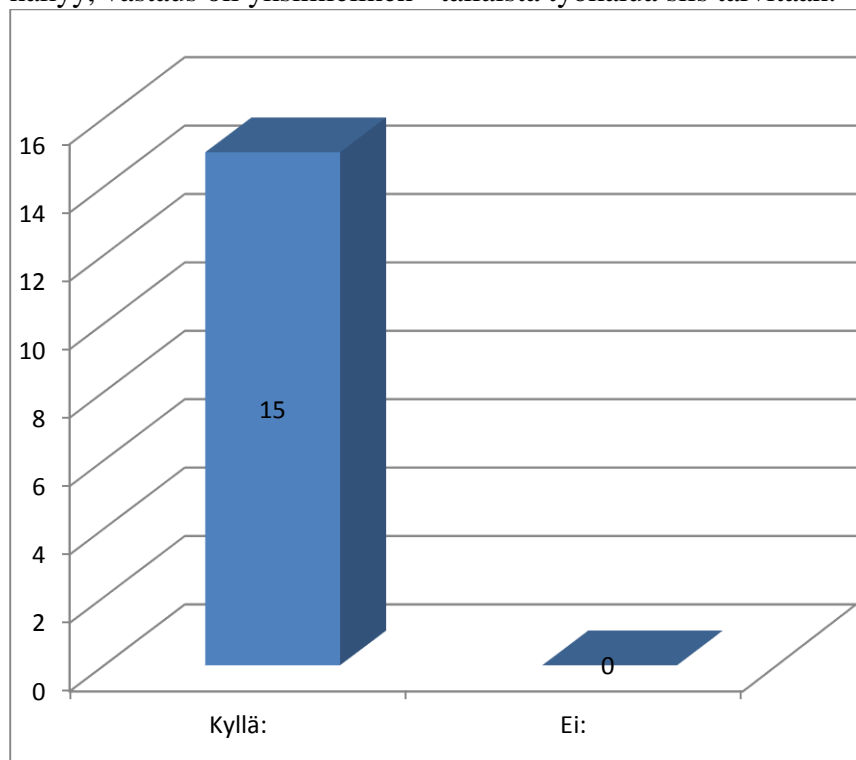
Kyselyyn kutsuttiin erikseen sähköpostitse 10 valikoitua henkilöä eri ryhmistä ja tiimeistä (verkonvalvonnasta, suunnittelusta ja niin edelleen). Tämän lisäksi kysely julkaistiin siten, että koko henkilöstö pystyi vastaamaan siihen. Kyselyyn osallistumiskynystä haluttiin madaltaa, jolloin annettiin mahdollisuus vastata nimettömänä. Kyselyyn vastasi yhteensä 15 asiantuntijaa.

Kahdeksan ensimmäistä kysymystä oli tehty niin, että asiantuntija pystyi valitsemaan useamman vaihtoehdon (paitsi ensimmäisessä kysymyksessä ainoastaan ”Kyllä/Ei”-vastaus) ja antamaan myös vapaan vastauksen. Kolmeen viimeiseen kysymykseen oli mahdollisuus muotoilla vastaus vapaasti. Viimeinen näistä kolmesta oli tarkoitettu osioksi, jossa asiantuntija pystyisi antamaan muita kommentteja tai kertoa omia ideoitaan.

Seuraavissa kappaleissa käsitellään kysymykset kyselyjärjestyksessä ja analysoidaan vastaukset lyhyesti, ja viimeisessä kappaleessa luodaan koko kyselyn perusteella muodostettavat vaatimukset, jotka siirretään osaksi vaatimusmäärittelyä.

Tarvitaanko automaattista konfiguraationhallintajärjestelmää?

Vastausvaihtoehdoiksi annettiin ”Kyllä” ja ”Ei”. Kuten oheisesta kuvaajasta (Kuvio 1) näkyy, vastaus oli yksimielinen - tällaista työkalua siis tarvitaan.



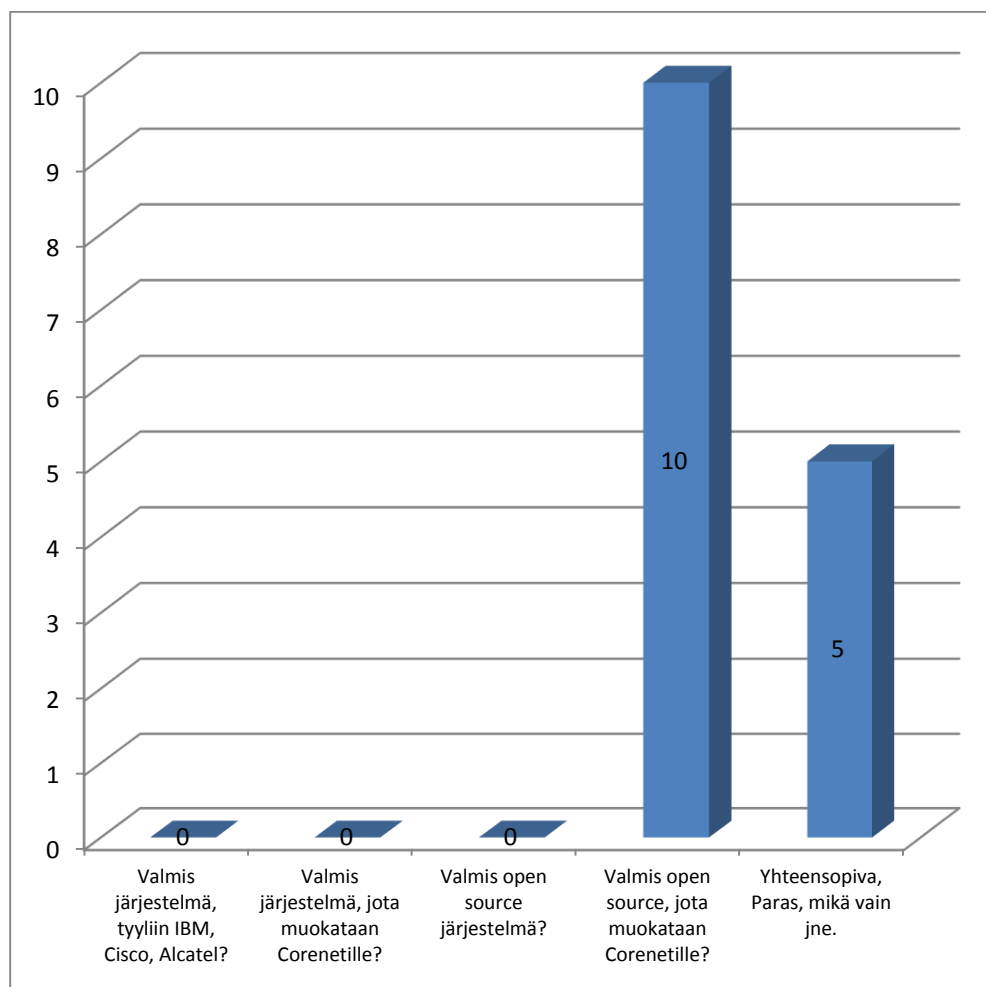
Kuvio 1. Vastaus oli yksimielinen

Millainen konfiguraatiohallintajärjestelmän tulisi olla?

Kysymys asetettiin lähinnä sillä ajatusmallilla, että etsittäisiin sopiva avoimeen lähdekoodiin pohjautuva ratkaisu, jota jatkokehitettäisiin Corenetin tarpeisiin. Lisäksi haluttiin kysyä asiantuntijoidenkin mielipidettä ja he olivat samaa mieltä.

Kukaan ei halunnut valmista, isojen valmistajien luomaa, hallintajärjestelmää edes muokkausmahdollisuudella. Pelkkä avoimen lähdekoodin ratkaisukaan ei ollut riittävä.

Muutamassa vastauksessa pidettiin oikeana vaihtoehtona sitä, mikä on vain hyvä, paras ja käytännöllisin, joka siis täyttää tarkoituksensa.



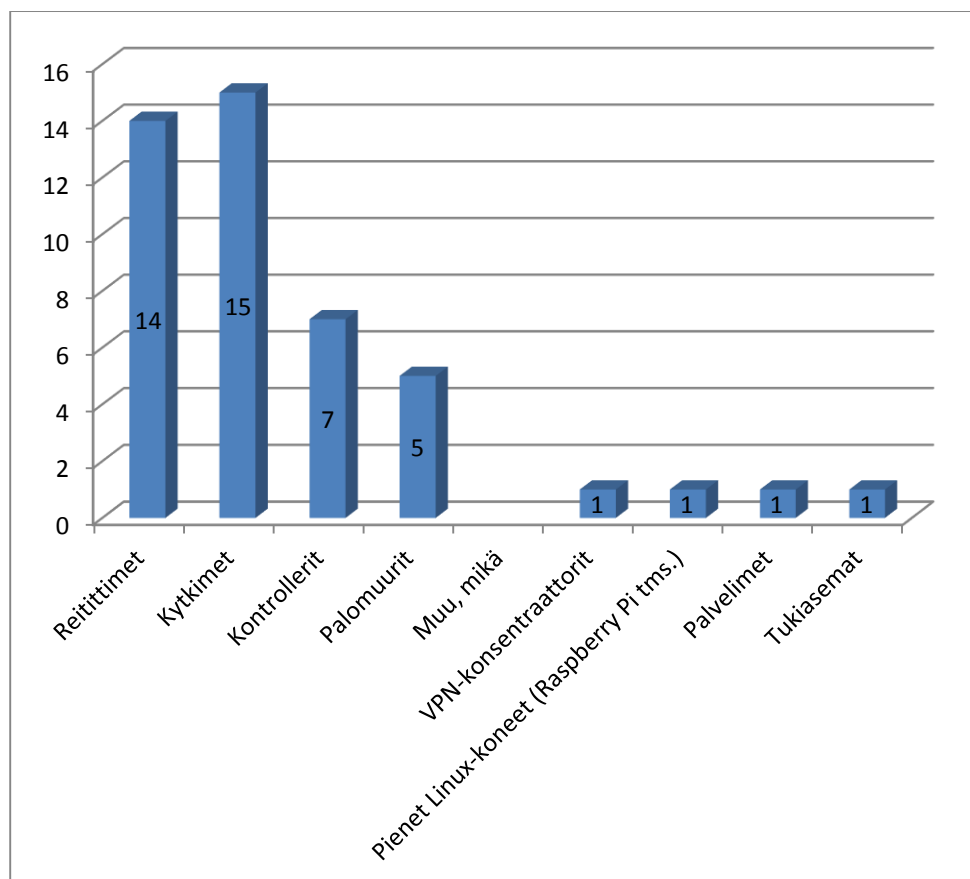
Kuvio 2. Millainen konfiguraatiohallintajärjestelmän tulisi olla?

Mitä eri laitteita konfiguraatiohallintajärjestelmän tulee tukea?

Corenetin verkkolaitteiden skaala on todella laaja, niin kuin tyypillisessä nykyaikaisessa tietoliikenneverkossa, ja erilaisia verkkolaitteita löytyy paljon. Tarvitseeko tulevan työkalun siis tukea kaikkia näitä eri laitteita ja laitetyppejä?

Vastauksista käy ilmi, että ennen kaikkea lähiverkkokytkimet tulisi olla tuettuna ja hyvänä kakkosena tulevat lähiverkon reitittimet. Nämä ovatkin ehkä juuri ne toiminnaltaan tärkeimmät ja lukumäärältään suurimmat verkkoelementit.

Kysymyksessä annettiin asiantuntijoille myös mahdollisuus antaa omia mielipiteitään/ideoitaan. Asiantuntijat esittivät neljä kappaletta muita vaihtoehtoja. Muista vaihtoehtoista voinee todeta, että palvelimia hallitaan omilla järjestelmillä ja nykyaikaisia tukiasemia hallitaan kontrollerin tai virtuaalisen kontrollerin avulla, mikä osaltaan voidaan rinnastaa lähiverkkokytkimeen.

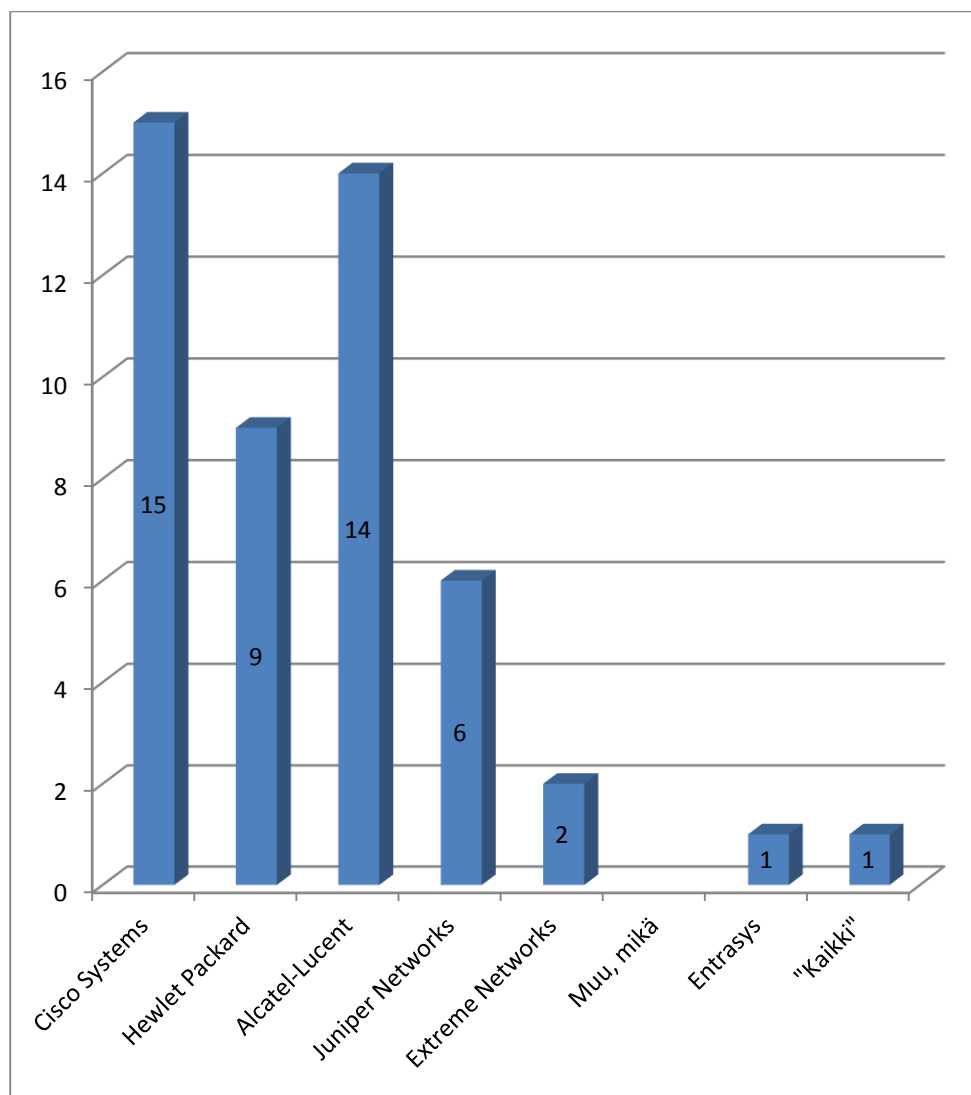


Kuvio 3. Mitä eri laitteita konfiguraatiohallintajärjestelmän tulee tukea?

Minkä valmistajan laitteita järjestelmän tulee tukea?

Nykyaikaisissa tietoliikenneverkossa on useiden eri laitetyyppien lisäksi usein käytetty myös eri laitevalmistajien laitteita. Asiantuntijat olivat sitä mieltä, että Cisco Systemsin ja Alcatel-Lucentin laitteet täytyisi ehdottomasti olla tuettuna. Loogista sinänsä, koska näiden laitevalmistajien laitteiden lukumäärät ovat Corenetin valvomissa ja ylläpitämissä verkoissa laajimmat. Hyvänä kakkosena tuli Hewlett-Packard.

Eräs asiantuntija ehdotti myös tukea Enterasysin laitteille (tukiasema / kontrolleri), ja yksi vastaus oli kaiken kattava, nimittäin ”kaikki”.



Kuvio 4. Minkä valmistajan laitteita järjestelmän tulee tukea?

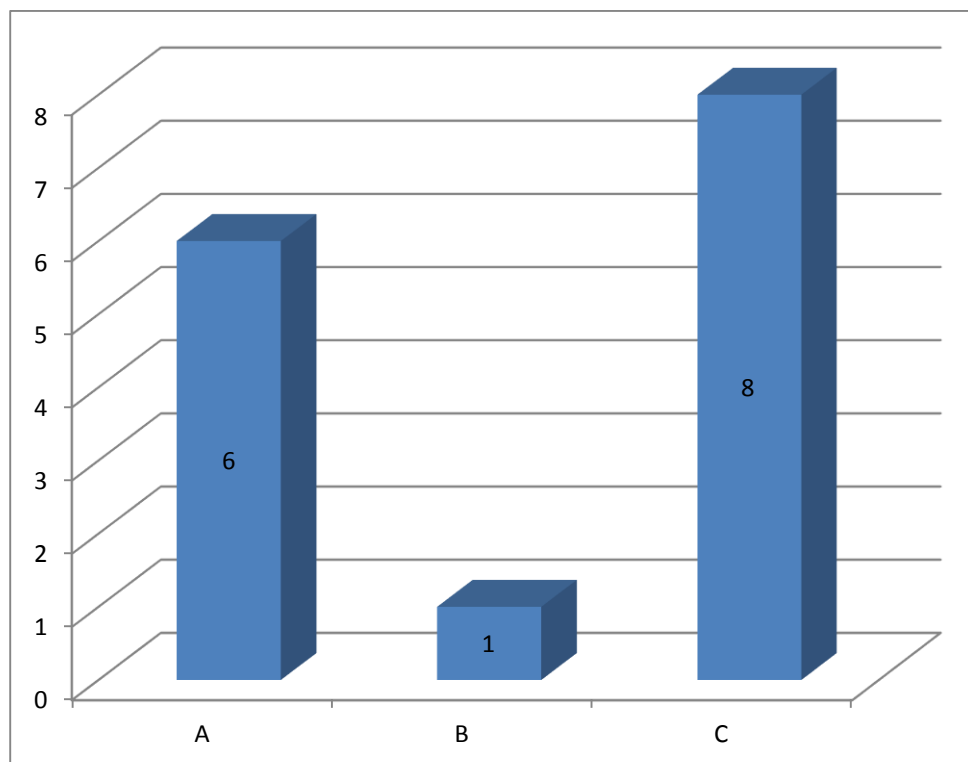
Miten toivoisit esi-/loppukonfiguraation tapahtuvan uusissa asennuksissa?

Seuraavaksi keskityttiin kyselemään tietoja liittyen itse konfiguraatioiden hallintaan. Tarkoituksena oli löytää vastaus siihen, miten laitteet tulisivat konfiguroida ennen lähettämistä sijoituspaikkaansa ja miten toimia, kun laitteet ovat ensimmäistä kertaa kytkettynä verkkoon ilman lopullista konfiguraatiota.

Vastausvaihtoehtoina annettiin kolme eri skenaariota:

- Skenaario A: ”Template-mallilla”, missä on valmiita kohdekohtaisia pohjia, joita muutetaan käsin tarpeen vaatiessa.
- Skenaario B: Manuaalisesti, kuten tähänkin asti
- Skenaario C: Ohjattu luominen (Wizard) (Haetaan pohja, jonka jälkeen kehote (prompti) kysyy pakolliset muutettavat arvot)

Huiksenhienon voiton vei Wizard-vaihtoehto eli pohjan lataamisen jälkeen kehote kysyi muutettavat arvot, kuten IP-osoitteen, järjestelmänimen (hostname), SNMP-tiedot. Hyvänä kakkosena tuli ”Template”-malli, jossa käytettäisiin valmiita, käsin muokattavia pohjia. Nykyisiä käytäntöjä piti parhaana yksi asiantuntija. Manuaalisella toiminnalla poistetaan muiden virheiden tapahtuminen, mutta inhimilliset erehdyksen mahdollisuus kasvaa suuremmaksi. Prosessin automatisointi säästäisi ainakin aikaa sekä luultavasti vähentäisi yksinkertaisimpien virheiden syntymistä.

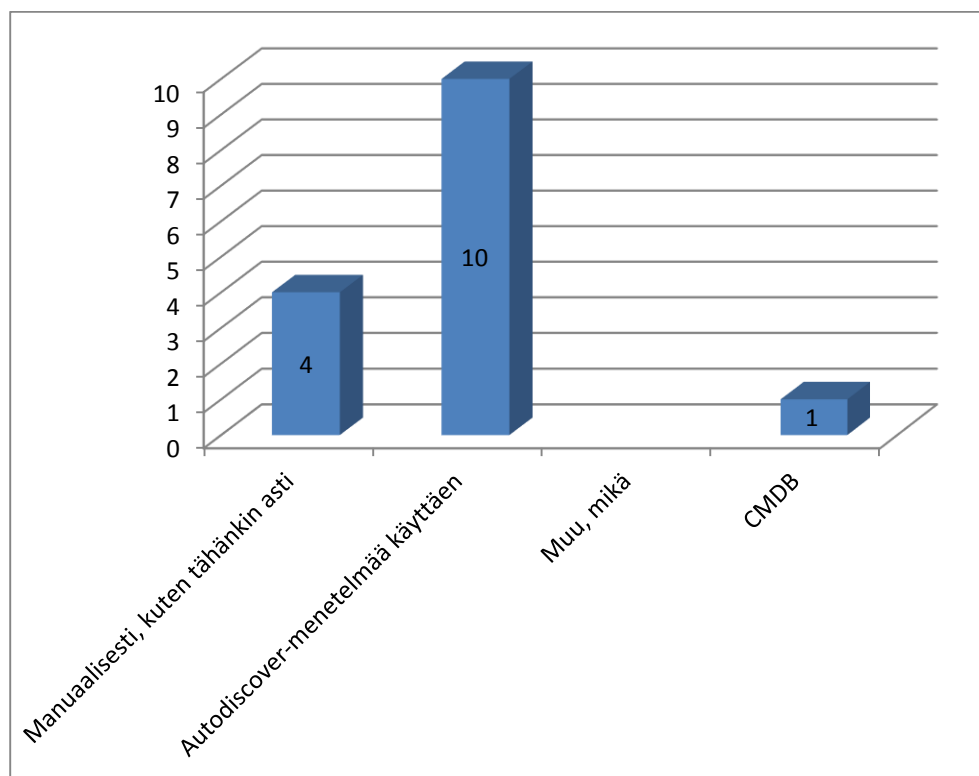


Kuvio 5. Miten toivoisit esi-/loppukonfiguraation tapahtuvan uusissa asennuksissa?

Miten uudet laitteet tulisi lisätä järjestelmään?

Seuraava kysymys koski verkkolaitteiden lisäämistä Corenetin konfiguraatiohallintajärjestelmään. Asiantuntijoille annettiin kahden vaihtoehdon lisäksi vapaus antaa oma kommenttinsa asiasta, mutta Autodiscovery – eli automaattinen lisäys, vei voiton. Työkalu siis tunnistaisi laitteen automaattisesti annettujen parametrien perusteella.

Osa asiantuntijoista (26 %) haluaisi pysyä nykyisessä mallissa ja yksi ehdotti konfiguraatiohallintatietokannan käyttöä (CMDB = Configuration management database). CMDB onkin tällä hetkellä käytössä, mutta laitteita ei lisätä siihen tällä hetkellä automaattisesti eikä se sisällä konfiguraatiotietoja kaikista laitteista.

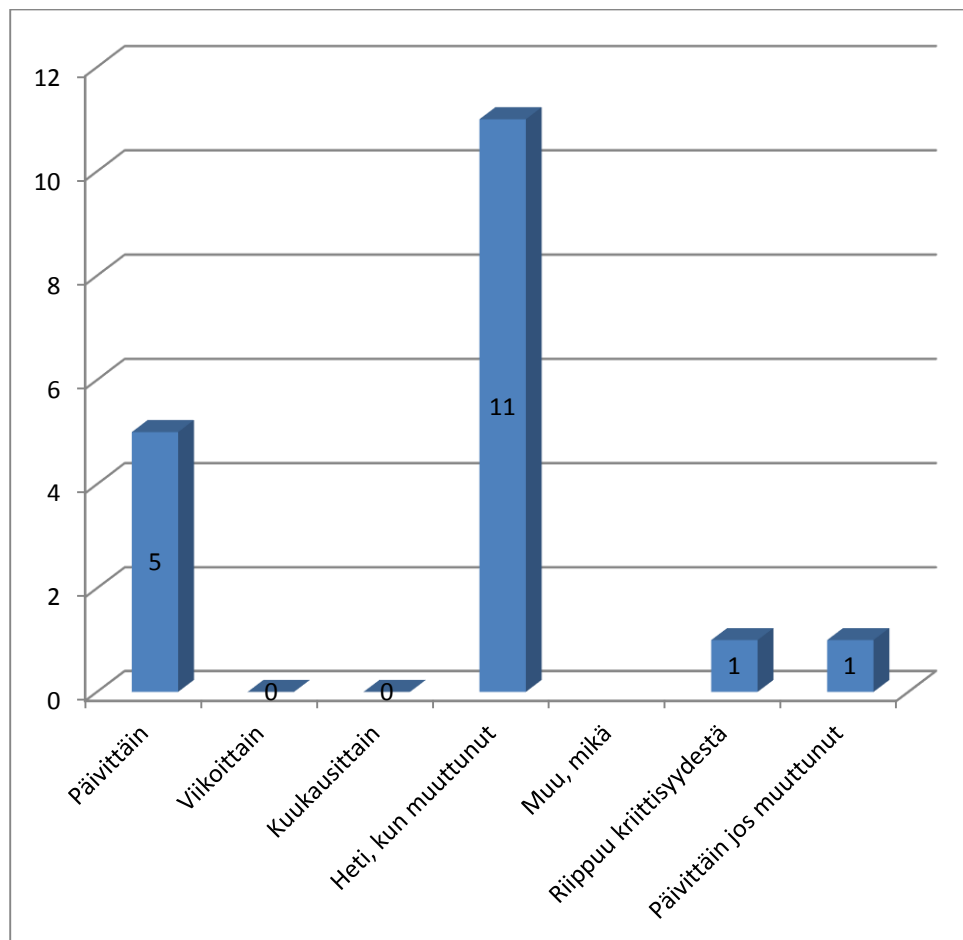


Kuvio 6. Miten uudet laitteet tulisi lisätä järjestelmään?

Millä syklillä laitteista otetaan varmuuskopio?

Varmuuskopiointi on ehdottoman tärkeää dynaamisessa verkossa. Verkkolaitteista on välttämätöntä ottaa varmuuskopiot, jotta vikatilanteen sattuessa selvittää laitevaihdolla ja uuteen laitteeseen saadaan varmasti tuorein konfiguraatio eikä koko laitetta tarvitse konfiguroida alusta loppuun käsin. Näin myös taataan se, että oikeat laiteportit ovat käytettävissä ja liitetty oikeisiin aliverkkoihin.

Osa asiantuntijoista oli sitä mieltä, että laitteista on otettava varmuuskopiot heti, kun konfiguraatio on muuttunut. Osa oli sitä mieltä, että päivittäin ja osa ehdotti molempia. Eräs asiantuntija ehdotti varmuuskopiointisyklin liitettäväksi laitteen kriittisyyteen ja yksi asiantuntija ehdotti varmuuskopiointia päivittäin, mikäli konfiguraatio on muuttunut. Aikaleimaperusteinen ratkaisu voisi olla hyvä, mutta haastava toteuttaa.



Kuvio 7. Millä syklillä laitteista otetaan varmuuskopio?

Miten tärkeäksi koet seuraavat asiat?

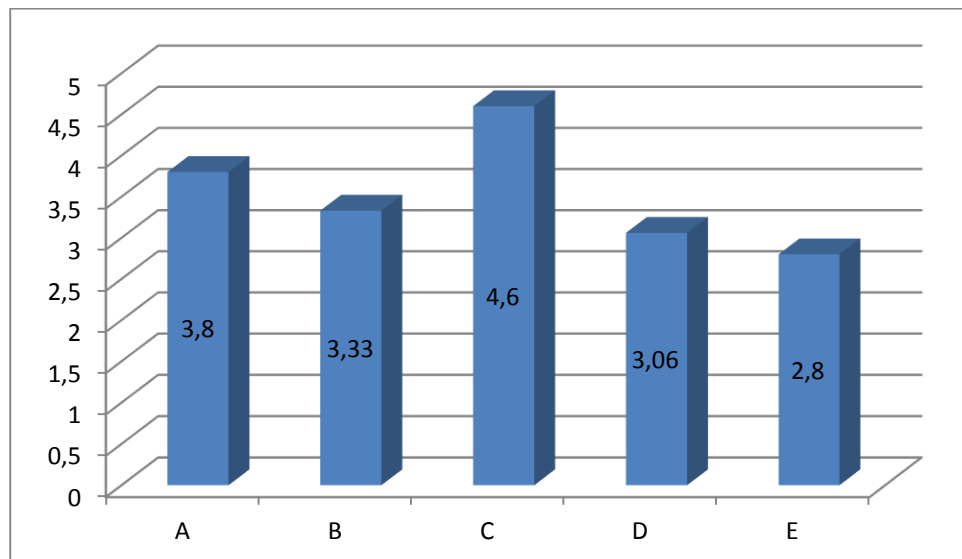
Tässä kohdassa asiantuntijoille annettiin viisi kysymystä, jotka heidän piti painottaa arvoilla 1-5, jossa 1 on ”ei tärkeää” ja 5 on ”erittäin tärkeää”.

Kyseessä olevat kohdat olivat:

- A. Konfiguraation poikkeavuustarkistus ennen varmuuskopion ottoa (jos ei muuttunut, ei varmuuskopiota)?
- B. Ilmoitus tiettyyn sähköpostiosoitteeseen ”vihamielisestä” muutoksesta?
- C. Auditti (kuka teki, mitä teki ja milloin teki?)
- D. Automaattinen laitteen ohjelmiston tarkistus/päivitys?
- E. Automaattinen roll-back (= palautetaan viimeksi toiminut konfiguraatio automaattisesti) ”vihamielisen” muutoksen tapahtuessa?

Tärkeimmäksi ominaisuudeksi nousi ”Audit”, eli tieto siitä, kuka teki, mitä teki ja milloin teki. Vähiten tärkeäksi koettiin automaattinen konfiguraation ”rollback” ”vihamielisen” muutoksen tapahtuessa. Tämän tyyppinen toiminta vaatisi lisäksi politiikkojen luomisen, jotta ”vihamieliset” muutokset tulee määriteltyä.

Muut kolme kohtaa koettiin suhteellisen tärkeiksi, keskiarvon jäädessä kolmosen yläpuolelle. Hajonta vaihtoehtojen kesken on pientä, joten kaikki on suhteellisesti ottaen oltava tuettuna.



Kuvio 8. Asioiden tärkeysjärjestyksellä on selkeät erot. Auditti on kirkkaasti tärkein.

2.5.2013

Mihin varmuuskopiot olisi mielestäsi hyvä siirtää laitteelta?

Tämä osio oli kaikille pakollinen. Tässä osiossa kartoitettiin asiantuntijoille mieluisinta paikkaa varmuuskopion säilyttämiselle, josta sen voisi tarvittaessa hakea.

Vastausten yhdenmukaisuuden johdosta tästä voisi vetää johtopäätöksen, että tarvitaan kahdennettu palvelin, joka voisi sijaita hallintaverkon sisä- tai ulkopuolella, ja johon on hoidettu pääsynhallinta.

Mitä muuta tulisi järjestelmää hankittaessa sinusta huomioida?

Tähänkin kysymykseen tuli antaa vapaamuotoinen vastaus.

Tärkeänä nähdään käytettävyys ja yksinkertaisuus, ja että se istuu käytettyjen prosessien ja itse työnteon tukemiseksi. Selkeästi valmistajalla ei ole väliä, kunhan se toimii ja sillä voisi hoitaa myös massakonfiguraatit.

Pitää eritellä, mikä voidaan automatisoida ja mikä jää manuaalisesti käsiteltäväksi. Lisenssimaksujen toivotaan jäävän minimiin, mikä on tarkoituskin.

Sana on vapaa - voit antaa muita mieleen juolahtaneita kommentteja.

Tämä osio ei ollut enää pakollinen, vaan tähän sai vapaasti kertoa mielipiteitään ja muita mieleen juolahtaneita kommentteja.

Kaikki annetut kommentit voidaan kiteyttää seuraavan laisesti: Testaus ja mahdollisten ”wizardien” ylläpito pitää huomioida valintaa tehtäessä.

Pikainen yhteenveto tuloksista

Vastauksista päätellen konfiguraatiohallintatyökalu on tarpeellinen, kaikki vastaajat ovat yksimielisesti tätä mieltä. Vastaajien mielestä mahdollinen ratkaisu tulisi pohjautua avoimeen lähdekoodiin, jota muokataan Corenetin tarpeiden mukaan toimivaksi.

Työkalun tulee tukea suurta määrää eri verkkolaitteita, vähintäänkin kytkimiä ja reitittimiä. Laittevalmistajista tulee olla edustettuna vähintään Cisco Systems ja Alcatel-Lucent. Lisäksi olisi hyvä säilyttää optio lisätä muita laitteita ja laitetoimittajia järjestelmän piiriin.

Esi- ja loppukonfiguroinnin Template-malli sai kannatusta 40 % ja ”Wizardi” 53 % eli hieman enemmän. ”Wizardi” vaihtoehtona herätti epäilyksiä ja aiheesta tulikin hyviä kommentteja. Vaihtoehto tähän toteutukseen on joko tai. Yksi asiantuntija halusi pitää tämän nykyisellään, eli täysin manuaalisina toimenpiteinä

Uusien laitteiden lisääminen tulisi tapahtua autodiscover-menetelmää käyttäen – optiona manuaalinen lisäys. Autodiscover sai noin 73 %:n kannatuksen.

Varmuuskopiot tulisi ottaa, kun konfiguraatio on muuttunut tai vaihtoehtoisesti päivittäin. Mikäli otetaan päivittäin, niin täytyy määritellä jokin raja, kuinka monta varmuuskopiota konfiguraatioista pidetään tallessa kerrallaan, ja milloin varmuuskopio vanhenee.

Tärkeysjärjestyksessä auditti oli tärkein elementti ja automaattista rollbackia ei pidetty niinkään suuressa arvossa. Yli kolmosen kipusivat myös ilmoitus vihamielisestä muutoksesta, konfiguraation poikkeavuuden tarkistus ja ohjelmiston tarkistus/päivitys.

Ehdottomat vaatimukset vastausten perusteella

- Avoimeen lähdekoodiin perustuva ratkaisu
- Laitetuki vähintään kytkimille ja reitittimille
- Työkalun täytyy tukea vähintään Cisco Systemsin ja Alcatel-Lucentin tarjoamia laitteita
- Autodiscover-menetelmän hyödyntäminen
- Varmuuskopiointisykli: päivittäin / heti, kun konfiguraatio on muuttunut
- Audit trail
- Ohjelmiston tarkistus / päivitys